VMware vRealize Log Insight-Benutzerhandbuch

vRealize Log Insight 2.5

Dieses Dokument unterstützt die aufgeführten Produktversionen sowie alle folgenden Versionen, bis das Dokument durch eine neue Auflage ersetzt wird. Die neuesten Versionen dieses Dokuments finden Sie unter http://www.vmware.com/de/support/pubs.

DE-001661-00



Die neueste technische Dokumentation finden Sie auf der VMware-Website unter:

http://www.vmware.com/de/support/

Auf der VMware-Website finden Sie auch die aktuellen Produkt-Updates.

Falls Sie Anmerkungen zu dieser Dokumentation haben, senden Sie Ihre Kommentare und Vorschläge an:

docfeedback@vmware.com

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

VMware Global, Inc.
Zweigniederlassung Deutschland
Freisinger Str. 3
85716 Unterschleißheim/Lohhof
Germany
Tel.: +49 (0) 89 3706 17000
Fax: +49 (0) 89 3706 17333
www.vmware.com/de

Inhalt

Informationen zum VMware vRealize Log Insight -Benutzerhandbuch

Das *VMware vRealize Log Insight-Benutzerhandbuch* enthält Informationen zur Nutzung der Web-Benutzeroberfläche von VMware® vRealize™ Log Insight™, einschließlich den Verfahren zum Filtern und Suchen von Protokollnachrichten, zum Durchführen von Analysen und zum Darstellen von Suchergebnissen sowie zur dynamischen Extrahierung von Feldern aus Protokollnachrichten basierend auf benutzerdefinierten Abfragen.

Zielgruppe

Diese Informationen sind für alle Log Insight-Benutzer hilfreich.

Verwenden von Log Insight

1

Log Insight bietet skalierbare Protokollzusammenfassung und Indizierung für die vCloud Suite, einschließlich aller Editionen von vSphere, mit Funktionen zur echtzeitnahen Suche und Analysefunktionen.

Log Insight sammelt, importiert und analysiert Protokolle für Antworten in Echtzeit auf Probleme in Bezug auf Systeme, Dienste und Anwendungen und leitet wichtige Einblicke ab.

Hochleistungsaufnahme

Log Insight kann alle Protokolltypen oder computergenerierten Daten verarbeiten. Log Insight unterstützt sehr hohe Durchsatzraten und niedrige Latenz. Log Insight akzeptiert über Syslog übermittelte Daten.

Skalierbarkeit

Log Insight ermöglicht eine horizontale Skalierung durch den Einsatz mehrerer virtueller Appliance-Instanzen. Dies ermöglicht eine lineare Skalierung des Aufnahmedurchsatzes, erhöht die Abfrageleistung und sorgt für Hochverfügbarkeit bei der Aufnahme. Im Cluster-Modus bietet Log Insight Master- und Worker-Knoten. Master- und Worker-Knoten sind für eine Teilmenge von Daten verantwortlich. Master-Knoten können alle Teilmengen von Daten abfragen und die Ergebnisse aggregieren.

Echtzeitnahe Suche

Über Log Insight erfasste Daten können innerhalb von Sekunden gesucht werden. Auch können historische Daten über dieselbe Schnittstelle mit derselben niedrigen Latenz gesucht werden.

Log Insight unterstützt komplexe Schlüsselwortabfragen. Schlüsselwörter sind als alphanumerische Zeichen, Bindestriche oder Unterstriche definiert. Neben den komplexen Schlüsselwortabfragen unterstützt Log Insight Glob-Abfragen (zum Beispiel erro?, vm*) und feldbasierte Filterung (zum Beispiel hostname does NOT match test*, IP contains "10.64"). Zudem können Protokollmeldungsfelder mit numerischen Werten zum Definieren von Auswahlfiltern verwendet werden (zum Beispiel CPU>80, 10<threads<100 usw.).

Suchergebnisse werden als einzelne Ereignisse dargestellt. Jedes Ereignis stammt aus einer einzelnen Quelle, Suchergebnisse können hingegen aus mehreren Quellen stammen. Sie können Log Insight zum Korrelieren der Daten in einer oder mehreren Dimensionen verwenden (zum Beispiel Zeit- und Anforderungsbezeichner) und somit eine kohärente Ansicht über den Stapel hinaus bieten. Auf diese Weise wird die Ursachenanalyse erheblich erleichtert.

Windows-Erfassungsagent

Log Insight verwendet einen nativen Windows Agent, um Protokolldaten über Windows-Server und -Desktops zu sammeln. Sie können Ereignisse über Windows-Ereigniskanäle und Protokolldateien erfassen und diese an den Log Insight-Server weiterleiten.

Intelligentes Gruppieren

Log Insight verwendet eine neue Technologie des maschinellen Lernens. Bei der intelligenten Gruppierung werden eingehende unstrukturierte Daten gescannt und umgehend nach Problemtyp in Meldungen gruppiert, damit Sie die Probleme in Ihren physischen, virtuellen und hybriden Cloud-Umgebungen schnell verstehen und analysieren können.

Zusammenfassung

Aus den Protokolldaten extrahierte Felder können für die Zusammenfassung verwendet werden. Diese Funktion ähnelt derjenigen der GROUP-BY-Abfragen in einer relationalen Datenbank oder in Pivot-Tabellen in Microsoft Excel. Der Unterschied ist, dass mit dieser Funktion keine Extrahierungs-, Umwandlungs- und Ladevorgänge (ETL) undLog Insight-Skalierungen jedweder Größe erforderlich sind.

Sie können Zusammenfassungsansichten der Daten generieren und spezifische Ereignisse oder Fehler identifizieren, ohne auf mehrere Systeme und Anwendungen innerhalb von Systemen und Anwendungen zugreifen zu müssen. Beispiel: Während der Anzeige einer wichtigen Systemmetrik, zum Beispiel die Anzahl der Fehler pro Minute, können Sie einen Drilldown zu einem bestimmten Zeitraum von Ereignissen durchführen und die in der Umgebung aufgetretenen Fehler untersuchen.

Laufzeit-Feldextraktion

Nicht formatierte Protokolldaten sind nicht immer leicht zu verstehen und möglicherweise müssen Sie einige Daten verarbeiten, um die Felder zu identifizieren, die für die Suche und Zusammenfassung wichtig sind. Log Insight enthält die Laufzeit-Feldextraktion zur Behebung dieses Problems. Durch Angabe eines regulären Ausdrucks können Sie jedes Feld dynamisch aus den Daten extrahieren. Die extrahierten Felder können zur Auswahl, Projektion und Zusammenfassung verwendet werden (ähnlich der Verwendung der Felder, die zum Zeitpunkt der Analyse extrahiert wurden).

Dashboards

Sie können Dashboards mit nützlichen Metriken erstellen, die Sie intensiv überwachen möchten. Jede Abfrage kann in ein Dashboard-Widget umgewandelt und für jeden Zeitbereich zusammengefasst werden. Sie können die Leistung Ihres Systems für die letzten fünf Minuten, die letzte Stunde oder den letzten Tag überprüfen. Sie können eine Aufschlüsselung der Fehler nach Stunde anzeigen und die Trends der Protokollereignisse beobachten.

Sicherheitsüberlegungen

IT-Entscheidungsträger, -Architekten und -Administratoren sowie andere Personen, die sich mit den Sicherheitskomponenten von Log Insight vertraut machen müssen, müssen das VMware vRealize Log Insight-Sicherheitshandbuch lesen.

Das Sicherheitshandbuch enthält kurz gefasste Hinweise auf die Sicherheitsmerkmale von Log Insight. Zu den behandelten Themen gehören unter anderem die externen Schnittstellen, Ports und Authentifizierungsmechanismen sowie die Möglichkeiten zur Konfiguration und Verwaltung der Sicherheitsfunktionen.

Dieses Kapitel behandelt die folgenden Themen:

Übersicht über die Web-Benutzeroberfläche von Log Insight

Auf welche Funktionalität Sie zugreifen können, hängt davon ab, welches Benutzerkonto Sie für die Anmeldung bei der Web-Benutzeroberfläche von Log Insight verwenden.

Die Registerkarte „Dashboards“

Die Registerkarte **Dashboards** enthält benutzerdefinierte Dashboards und Inhaltspaket-Dashboards. Auf der Registerkarte **Dashboards** können Sie Diagramme der Protokollereignisse in Ihrer Umgebung anzeigen oder eigene benutzerdefinierte Widgets erstellen, um die Informationen aufzurufen, die für Sie am relevantesten sind.

Die Registerkarte „Interaktive Analyse“

Auf der Registerkarte **Interaktive Analyse** können Sie Protokollereignisse suchen und filtern, und Sie können Abfragen erstellen, um Ereignisse aufgrund von Zeitstempel, Text, Quelle und Feldern in Protokollereignissen zu extrahieren. Log Insight zeigt die Abfrageergebnisse in Diagrammform an. Sie können diese Diagramme speichern, um sie später auf der Registerkarte **Dashboards** anzusehen.

Inhaltspakete

Inhaltspakete enthalten Dashboards, extrahierte Felder, gespeicherte Abfragen und Warnungen, die sich auf ein bestimmtes Produkt oder auf eine Gruppe von Protokollen beziehen. Sie können die Inhaltspakete über das Dropdown-Menü oben rechts in der Web-Benutzeroberfläche von Log Insight aufrufen.

Inhaltspakete können von Log Insight-Benutzern importiert oder erstellt werden. Weitere Informationen hierzu finden Sie unter „Arbeiten mit Inhaltspaketen“, auf Seite 32.

Die Benutzeroberfläche für Administratoren

Log Insight-Administratoren können Benutzerkonten verwalten, Speicherorte und Archivierung konfigurieren, einen SMTP-Server für ausgehende E-Mail-Benachrichtigungen konfigurieren und diverse andere Parameter ändern. Das URL-Format der Benutzeroberfläche für Administratoren lautet https://*log_insight-host*/admin/, wobei *log_insight-host* die IP-Adresse oder der Hostname der virtuellen Log Insight-Appliance ist.

Suchen und Filtern von Protokollereignissen

Sie können Protokollereignisse auf der Registerkarte **Interaktive Analyse** suchen und filtern.

Sie können beliebige vollständige Schlüsselwörter, Globs oder Ausdrücke in das Suchtextfeld eingeben und auf **Suchen** klicken, um nur Ereignisse zu finden, die die angegebenen Schlüsselwörter enthalten.

Sie können den Zeitraum auf einer der Seiten **Dashboards** oder **Interaktive Analyse** in der Web-Benutzeroberfläche angeben. Die Zeiträume sind beim Filtern einschließend.

Sie können nach Protokollereignissen suchen, die mit bestimmten Werten von bestimmten Feldern übereinstimmen. Wenn Sie den Text im Hauptsuchfeld in Anführungszeichen setzen, werden exakte Übereinstimmungen mit dem Ausdruck gesucht. Wenn Sie ein Leerzeichen in das Hauptsuchfeld eingeben, fungiert dieses als logischer UND-Operator. Die Suche verwendet nur vollständige Token: Wenn Sie z. B. den Suchbegriff „err“ eingeben, werden keine Übereinstimmungen mit „error“ ausgegeben.

Zur Angabe der Feldsuchkriterien oder Filter können Sie die Dropdown-Menüs und das Textfeld über der Liste der Protokollereignisse verwenden.

Innerhalb eines Filters für eine einzelne Zeile können Sie durch Kommas getrennte Werte eingeben, um ODER-Filter aufzulisten. Wählen Sie beispielsweise **Hostname enthält** und geben Sie `127.0.0.1, 127.0.0.2` ein. Die Suche gibt Ereignisse aus, die den Hostnamen 127.0.0.1 oder 127.0.0.2 enthalten.

HINWEIS Der Filter **Text enthält** behandelt jeden durch Komma getrennten Wert als ein vollständiges Schlüsselwort.

Sie können mehrere Feldfilter kombinieren, indem Sie eine neue Filterzeile für jedes Feld erstellen. Sie können den Operator, der auf mehrzeilige Filter angewandt wird, umschalten.

- Wählen Sie **Alle**, um den UND-Operator anzuwenden.
- Wählen Sie **Alle**, um den ODER-Operator anzuwenden.

HINWEIS Unabhängig von dem Umschaltwert ist der Operator für durch Kommas getrennte Werte innerhalb einer Einzelfilterzeile immer ODER.

Sie können Globs in Suchbegriffen verwenden, beispielsweise vm* oder vmw?re.

- Verwenden Sie * für 0 oder mehr Zeichen.
- Verwenden Sie ? für ein Zeichen.

HINWEIS Globs können nicht als erstes Zeichen eines Suchbegriffs verwendet werden. Beispielsweise können Sie 192.168.0.*in Ihren Filterabfragen verwenden, nicht aber *.168.0.0.

Informationen in Protokollereignissen

Sie können Protokolle in Log Insight mithilfe von Syslog aufnehmen.

Jedes Ereignis enthält die folgenden Informationen:

Typ	Beschreibung
Zeitstempel	Der Zeitpunkt, zu dem das Ereignis eingetreten ist.
Quelle	Die Herkunft des Ereignisses. Dies könnte der Ersteller der Syslog-Meldungen sein, z. B. ein ESXi-Host, oder eine Weiterleitung, z. B. ein Syslog-Aggregator.
Text	Der Rohtext des Ereignisses.
Felder	Ein Name-Wert-Paar, das aus dem Ereignis extrahiert wurde.

HINWEIS Log Insight ist nicht für den Inhalt der Protokollmeldungen von anderen VMware-Produkten verantwortlich. Bei Fragen zu den Protokollinhalten wenden Sie sich an das Produktteam, das die Protokollmeldung generiert hat.

Gruppieren von Ereignistypen

Log Insight verwendet das maschinelle Lernen, um ähnliche Ereignisse zu gruppieren. Die Gruppierung nach Ereignistypen vereinfacht die Fehlersuche und -behebung und die Analyse von Grundursachen.

Wenn Sie Abfragen in Log Insight ausführen, hängt die Anzahl der Ergebnisse von der Abfrage und vom Zeitraum ab. Oft geben Abfragen eine große Zahl an Ergebnissen aus. Das maschinelle Lernen sorgt für das dynamische Lernen und Anpassen von Mustern aus Ereignissen, die bei Log Insight eingehen.

Die Registerkarte **Ereignistypen** befindet sich auf der Seite „Interaktive Analyse“ unter der Suchleiste. Wenn Sie auf die Registerkarte **Ereignistypen** klicken, sehen Sie eine Liste ähnlicher Ereignisse, die in Gruppen zusammengefasst sind.

Das maschinelle Lernen analysiert Ereignisse und erfasst die Arten von Feldern, die in ähnlichen Protokollmeldungen enthalten sind. Beispiel: Ereignistypen können Zeitstempel, Zeichenfolge, Int, Hex und andere sein. Die erfassten Typen werden in der Liste **Ereignistypen** als Hyperlinks angezeigt.

Jeder vom maschinellen Lernen erfasste Typ stellt einen neuen Feldtyp, Smart-Feld genannt, dar. Der Standardname eines Smart-Felds folgt dem Format „Smart-Feld – *Typ Zahl* [*event_type*]“. Sie können den Standardnamen eines Smart-Felds ändern. Nachdem Sie ein Smart-Feld benannt haben, wird es wie andere Felder im Bereich „Felder“ angezeigt. Sie können ein Smart-Feld umbenennen oder löschen, aber Sie können seine Definition nicht ändern.

Das maschinelle Lernen führt ein neues statisches Feld, event_type, ein. Sie können den event_type als Filter zum Ein- oder Ausschließen bestimmter Ereignistypen bei Abfragen verwenden.

Filtern von Protokollereignissen nach Zeitraum

Sie können Protokollereignisse filtern, um nur die Ereignisse in einem bestimmten Zeitraum anzuzeigen.

Sie können den Zeitraum auf einer der Seiten **Dashboards** oder **Interaktive Analyse** in der Web-Benutzeroberfläche angeben. Die Zeiträume sind beim Filtern einschließend.

Voraussetzungen

Vergewissern Sie sich, dass Sie bei der Web-Benutzeroberfläche von Log Insight angemeldet sind. Das URL-Format lautet https://*log_insight-host*, wobei *log_insight-host* die IP-Adresse oder der Hostname der virtuellen Log Insight-Appliance ist.

Vorgehensweise

1. Wählen Sie im Dropdown-Menü links von der Schaltfläche **Suchen** einen der vordefinierten Zeiträume aus.
2. (Optional) Wählen Sie **Benutzerdefinierter Zeitraum**, wenn Sie den Anfangs- und Endpunkt des Zeitraums individuell festlegen möchten.

Suchen nach Protokollereignissen, die ein vollständiges Schlüsselwort enthalten

Sie können nach Protokollereignissen suchen, die ein vollständiges Schlüsselwort enthalten. Schlüsselwörter enthalten alphanumerische Zeichen, Bindestrich und Unterstrich.

Voraussetzungen

Vergewissern Sie sich, dass Sie bei der Web-Benutzeroberfläche von Log Insight angemeldet sind. Das URL-Format lautet https://*log_insight-host*, wobei *log_insight-host* die IP-Adresse oder der Hostname der virtuellen Log Insight-Appliance ist.

Vorgehensweise

1 Rufen Sie die Registerkarte **Interaktive Analyse** auf.

2 Geben Sie im Suchtextfeld das vollständige Schlüsselwort ein, nach dem Sie in den Protokollereignissen suchen möchten, und klicken Sie auf die Schaltfläche **Suchen**.

Protokollereignisse, die das angegebene vollständige Schlüsselwort enthalten, werden in der Liste angezeigt.

Die Zeichenfolge, nach der Sie gesucht haben, wird gelb hervorgehoben.

Weiter

Sie können die aktuelle Abfrage speichern, um sie später zu laden.

Suchen von Protokollereignissen nach Feldvorgängen

Mit der Liste der vorhandenen Felder können Sie Protokollereignisse mit bestimmten Werten nach einem Feld durchsuchen.

Wichtig Log Insight indiziert vollständige Begriffe, alphanumerische Begriffe, Bindestrich und Unterstrich.

Voraussetzungen

Vergewissern Sie sich, dass Sie bei der Web-Benutzeroberfläche von Log Insight angemeldet sind. Das URL-Format lautet https://*log_insight-host*, wobei *log_insight-host* die IP-Adresse oder der Hostname der virtuellen Log Insight-Appliance ist.

Vorgehensweise

1 Rufen Sie die Registerkarte **Interaktive Analyse** auf.

2 Klicken Sie auf **Filter hinzufügen**.

3 Wählen Sie in der Filterzeile unter dem Suchtextfeld im ersten Dropdown-Menü ein beliebiges definiertes Feld innerhalb von Log Insight aus.

   Beispiel: **hostname**.

   Die Liste enthält alle definierten Felder, die statisch verfügbar sind, Inhaltspaketen und in benutzerdefiniertem Inhalt. Abgesehen vom Feld **Text** sind alle Felder nach Namen sortiert. Da **Text** ein Sonderfeld ist, das auf den Text der Meldung verweist, wird **Text** oben in der Liste angezeigt und ist standardmäßig ausgewählt.

   Hinweis Numerische Felder enthalten zusätzliche Operatoren, die in Zeichenfolgenfeldern nicht vorkommen: =, >, <, >=, <=. Diese Operatoren führen numerische Vergleiche aus. Durch ihre Verwendung können andere Ergebnisse als bei der Verwendung von Zeichenfolgenoperatoren erzielt werden. Beispiel: Der Filter **response_time = `02`** ergibt als Treffer ein Ereignis, das ein Feld **response_time** mit einem Wert von 2 enthält. Der Filter **response_time enthält `02`** ergibt nicht denselben Treffer.

   ---

4 Wählen Sie in der Filterzeile unter dem Suchtextfeld mit dem zweiten Dropdown-Menü den Vorgang aus, der auf das im ersten Dropdown-Menü gewählte Feld angewandt werden soll.

   Wählen Sie zum Beispiel **enthält**. Der Filter **enthält** gleicht vollständige Token ab: Wenn Sie z. B. den Suchbegriff „err“ eingeben, werden keine Übereinstimmungen mit „error“ ausgegeben.

5 Geben Sie im Textfeld rechts neben dem Dropdown-Menü für den Filter den Wert ein, den Sie als Filter verwenden möchten.

   Sie können mehrere Werte durch Kommata getrennt auflisten. Der Operator zwischen diesen Werten ist ODER.

   HINWEIS Das Textfeld ist nicht verfügbar, wenn Sie im zweiten Dropdown-Menü den Operator **ist vorhanden** auswählen.

6 (Optional) Klicken Sie auf **Filter hinzufügen**, um weitere Filter hinzuzufügen.

   Oberhalb der Filterzeilen wird eine Umschaltfläche angezeigt.

7 (Optional) Wählen Sie für mehrere Filterzeilen den Operator zwischen den Filtern aus.

Option	Beschreibung
allen	Auswählen, um den UND-Operator zwischen Filterzeilen anzuwenden
alle	Auswählen, um den ODER-Operator zwischen Filterzeilen anzuwenden

   Standardmäßig ist **alle** gewählt.

8 Klicken Sie auf die Schaltfläche **Suchen**.

Beispiel: Suchen einer Gruppe von Hosts, deren Namen eine gemeinsame Zeichenfolge enthalten

Nehmen Sie an, Sie haben mehrere Hosts, darunter einen mit dem Namen w1-stvc-205-prod3 und einen anderen mit dem Namen w1-stvc-206-prod5.

Um alle Protokolle für beide Hosts zu finden, erstellen Sie die folgende Abfrage:

1 Lassen Sie das Suchtextfeld frei.

2 Definieren Sie den Filter.

   a Wählen Sie **Hostname** aus dem Dropdown-Menü „Feld“.

   b Wählen Sie **beginnt mit** aus dem Dropdown-Menü „Operator“.

   c Geben Sie **`w1-stvc`** in das Wert-Textfeld ein.

   Stattdessen können Sie auch den Operator **enthält** verwenden, aber dann müssen Sie im Suchwert einen Glob verwenden. Bei diesem Beispiel müssen Sie **`w1-stvc-*`** in das Wert-Textfeld eingeben.

3 Klicken Sie auf die Schaltfläche **Suchen**.

Weiter

Sie können die aktuelle Abfrage speichern, um sie später zu laden.

Suchen nach Ereignissen, die vor, nach oder während eines Ereignisses aufgetreten sind

Sie können die Liste der Protokollereignisse nach Ereignissen durchsuchen, die vor, nach und in der zeitlichen Umgebung eines Ereignisses in der Liste aufgetreten sind.

Wenn Sie mehr über den Status Ihrer Umgebung vor und nach einem Ereignis erfahren möchten, können Sie die umgebenden Ereignisse überprüfen.

Voraussetzungen

Vergewissern Sie sich, dass Sie bei der Web-Benutzeroberfläche von Log Insight angemeldet sind. Das URL-Format lautet https://*log_insight-host*, wobei *log_insight-host* die IP-Adresse oder der Hostname der virtuellen Log Insight-Appliance ist.

Vorgehensweise

1. Suchen Sie auf der Registerkarte **Interaktive Analyse** das Ereignis in der Liste.
2. Klicken Sie links neben der Ereigniszeile auf ⚙ und wählen Sie **Zeitraum ab diesem Ereignis festlegen** aus.
3. Wählen Sie im Dialogfeld „Zeitraum ab Ereignis festlegen“ mit den Dropdown-Menüs den Zeitraum und die Richtung des Zeitraums aus.

   Sie können aus einer Liste vordefinierter Zeiträume von 1 Sekunde bis 10 Minuten auswählen.
4. Klicken Sie auf **Zeitraum einstellen**.

Die Ereignisse, die in der zeitlichen Umgebung des ausgewählten Ereignisses auftreten, werden in der Liste angezeigt.

Hinweis Mit diesem Vorgang werden alle zuvor angegebenen Suchparameter und Filter gelöscht.

Anzeigen eines Ereignisses im Kontext

Sie können den Kontext eines Protokollereignisses anzeigen und die Protokollereignisse, die davor und danach eingetroffen sind, durchsuchen.

Wenn Sie mehr über den Status Ihrer Umgebung vor und nach einem Ereignis erfahren möchten, können Sie die umgebenden Ereignisse überprüfen.

Voraussetzungen

Vergewissern Sie sich, dass Sie bei der Web-Benutzeroberfläche von Log Insight angemeldet sind. Das URL-Format lautet https://*log_insight-host*, wobei *log_insight-host* die IP-Adresse oder der Hostname der virtuellen Log Insight-Appliance ist.

Vorgehensweise

1. Suchen Sie auf der Registerkarte **Interaktive Analyse** das Ereignis in der Liste.
2. Klicken Sie links neben der Ereigniszeile auf ⚙ und wählen Sie **Ereignis im Kontext anzeigen** aus.
3. (Optional) Scrollen Sie bis zum Fensterrand hoch oder herunter, um weitere Ereignisse zu laden.
4. (Optional) Klicken Sie auf den violetten Zeitstempel, um zurück zur markierten Meldung zu scrollen.
5. (Optional) Klicken Sie zum Hinzufügen von Filtern ganz oben auf **Filter hinzufügen** oder klicken Sie auf ein Feld im markierten Ereignis.
6. (Optional) Fügen Sie bestimmte Ereignistypen hinzu bzw. entfernen Sie sie, indem Sie auf ein Ereignis zeigen und dann auf ⚙ klicken.

Analysieren von Ereignistrends

Sie können Protokollereignisse für Trends und Anomalien analysieren.

Voraussetzungen

Vergewissern Sie sich, dass Sie bei der Web-Benutzeroberfläche von Log Insight angemeldet sind. Das URL-Format lautet https://*log_insight-host*, wobei *log_insight-host* die IP-Adresse oder der Hostname der virtuellen Log Insight-Appliance ist.

Vorgehensweise

1. Rufen Sie die Registerkarte **Interaktive Analyse** auf.

2 Erstellen Sie Ihre Abfrage mithilfe des Textfelds „Suchen“ und unter Anwendung von Filtern und führen Sie sie entsprechend aus.

3 Wählen Sie im Dialogfeld „Zeitraum ab Ereignis festlegen“ mit den Dropdown-Menüs den Zeitraum und die Richtung des Zeitraums aus.

4 Klicken Sie auf die Registerkarte **Ereignistrends**.

   Log Insight vergleicht Ihre Abfrage mit demselben Zeitraum unmittelbar zuvor und zeigt die Ergebnisse an.

Löschen aller Filterregeln

Sie können die Filter und Suchergebnisse löschen, um die Liste mit allen Protokollereignissen anzuzeigen.

Nachdem Sie eine Suche in der Ereignisliste durchgeführt haben, werden die Suchergebnisse auf dem Bildschirm angezeigt, bis Sie alle Abfragen löschen.

Voraussetzungen

Vergewissern Sie sich, dass Sie bei der Web-Benutzeroberfläche von Log Insight angemeldet sind. Das URL-Format lautet https://*log_insight-host*, wobei *log_insight-host* die IP-Adresse oder der Hostname der virtuellen Log Insight-Appliance ist.

Vorgehensweise

1 Entfernen Sie alle Filter auf der Registerkarte **Interaktive Analyse**.

2 Wenn im Suchtextfeld Text angezeigt wird, löschen Sie ihn.

3 Klicken Sie auf die Schaltfläche **Suchen**.

Beispiele für Suchanfragen

Sie können diese Beispiele beim Aufbau Ihrer Anfragen auf der Registerkarte **Interaktive Analyse** von Log Insight verwenden.

Beispiel: Abfrage aller Heartbeat-Ereignisse, die vom ESX/ESXi-hostd-Prozess gestern von 9:00 bis 10:00 Uhr gemeldet wurden

---

WICHTIG Log Insight indiziert vollständige Begriffe, alphanumerische Begriffe, Bindestrich und Unterstrich.

So fragen Sie alle Heartbeat-Ereignisse ab, die vom ESX/ESXi-hostd-Prozess gemeldet wurden:

1 Geben Sie im Suchfeld den Suchbegriff **`heartbeat*`** ein.

2 Definieren Sie einen Filter.

   a Wählen Sie **appname** aus dem ersten Dropdown-Menü.

   b Wählen Sie **enthält** aus dem zweiten Dropdown-Menü.

   c Geben Sie **`hostd`** in das Wert-Textfeld ein.

3 Definieren Sie den Zeitraum.

   a Wählen Sie im Dropdown-Menü **Zeitraum** die Option **Benutzerdefiniert**.

   b Geben Sie im ersten Textfeld das gestrige Datum und die Uhrzeit 9:00 Uhr ein.

   c Geben Sie im zweiten Textfeld das gestrige Datum und die Uhrzeit 10:00 Uhr ein.

4 Klicken Sie auf die Schaltfläche **Suchen**.

Beispiel: Suchen einer Gruppe von Hosts, deren Namen eine gemeinsame Zeichenfolge enthalten

Nehmen Sie an, Sie haben mehrere Hosts, darunter einen mit dem Namen w1-stvc-205-prod3 und einen anderen mit dem Namen w1-stvc-206-prod5.

Um alle Protokolle für beide Hosts zu finden, erstellen Sie die folgende Abfrage:

1 Lassen Sie das Suchtextfeld frei.
2 Definieren Sie den Filter.
   a Wählen Sie **Hostname** aus dem Dropdown-Menü „Feld“.
   b Wählen Sie **beginnt mit** aus dem Dropdown-Menü „Operator“.
   c Geben Sie **`w1-stvc`** in das Wert-Textfeld ein.

   Stattdessen können Sie auch den Operator **enthält** verwenden, aber dann müssen Sie im Suchwert einen Glob verwenden. Bei diesem Beispiel müssen Sie **`w1-stvc-*`** in das Wert-Textfeld eingeben.
3 Klicken Sie auf die Schaltfläche **Suchen**.

Beispiel: Abfrage aller Fehler, die von vCenter Server-Aufgaben, -Ereignissen und -Warnungen gemeldet wurden

So fragen Sie alle Fehler ab, die von vCenter Server-Aufgaben, -Ereignissen und -Warnungen gemeldet wurden:

1 Geben Sie im Suchfeld den Suchbegriff **`error`** ein.
2 Definieren Sie einen Filter.
   a Wählen Sie **vc_event_type** aus dem ersten Dropdown-Menü.
   b Wählen Sie den Operator **ist vorhanden** aus dem zweiten Dropdown-Menü aus.
3 Klicken Sie auf die Schaltfläche **Suchen**.

Beispiel: Abfrage der von ESX/ESXi gemeldeten SCSI-Latenz über 1 Sekunde

So fragen Sie die von ESX/ESXi gemeldete SCSI-Latenz über 1 Sekunde ab:

1 Geben Sie im Suchfeld den Suchbegriff **`scsi latency "performance has"`** ein.
2 Definieren Sie einen Filter.
   a Wählen Sie **vmw_vob_component** aus dem ersten Dropdown-Menü.
   b Wählen Sie den Operator **enthält** aus dem zweiten Dropdown-Menü aus.
   c Geben Sie **`scsiCorrelator`** in das Textfeld ein.
3 Definieren Sie einen zweiten Filter.
   a Wählen Sie **vmw_latency_in_micros** aus dem ersten Dropdown-Menü.
   b Wählen Sie den Operator **>** aus dem zweiten Dropdown-Menü aus.
   c Geben Sie **`1000000`** in das Textfeld ein.
4 Klicken Sie auf die Schaltfläche **Suchen**.

Beispiele für reguläre Ausdrücke

Sie können reguläre Ausdrücke in Textfelder eingeben, damit die Feldwerte Felder aus Protokollereignissen extrahieren.

Die eingegebenen Ausdrücke müssen die Java-Syntax für reguläre Ausdrücke beachten.

Tabelle 1-1. Zeichenoperatoren

Regulärer Ausdruck	Beschreibung
\	Wechselt zu einem Sonderzeichen
\b	Wortgrenze
\B	Keine Wortgrenze
\d	Eine Ziffer
\D	Eine Nichtziffer
\n	Neue Zeile
\r	Rückgabezeichen
\s	Ein Leerzeichen
\S	Ein beliebiges Zeichen außer Leerzeichen
\t	Registerkarte
\w	Ein alphanumerisches Zeichen oder ein Unterstrichzeichen
\W	Ein Zeichen, das weder ein alphanumerisches Zeichen noch ein Unterstrichzeichen ist

Beispiel: Sie wenden die folgenden regulären Ausdrücke auf die Zeichenfolge `1234–5678` an:

Regulärer Ausdruck	Ergebnis
\d	1
\d+	1234
\w+	1234
\S	1234-5678

Tabelle 1-2. Quantifizierer-Operatoren

Regulärer Ausdruck	Beschreibung
.	Ein beliebiges Zeichen außer neue Zeile
*	Null oder mehr Zeichen so lang wie möglich
?	Null oder ein Zeichen ODER so kurz wie möglich
+	Ein(e) oder mehrere
{<n>}	Genau <n> Mal
{<n>,<m>}	<n> bis <m> Mal

Beispiel: Sie wenden die folgenden regulären Ausdrücke auf die Zeichenfolge `aaaaa` an:

Regulärer Ausdruck	Ergebnis
.	a
*	aaaaa

Regulärer Ausdruck	Ergebnis
.*?	aaaaa
.{1}	a
.{1,2}	aa

Tabelle 1-3. Kombinationsoperatoren

Regulärer Ausdruck	Beschreibung
.*	Alle
.*?	Alle möglichst kurzen vor

Beispiel: Sie wenden die folgenden regulären Ausdrücke auf die Zeichenfolge `a b 3 hi d hi` an:

Regulärer Ausdruck	Ergebnis
a.* hi	b 3 hi d
a .*? hi	b 3

Tabelle 1-4. Logische Operatoren

<table>
<tr><th>Regulärer Ausdruck</th><th>Beschreibung</th></tr>
<tr><td>^</td><td>Anfang einer Zeile ODER nicht, wenn in Klammern</td></tr>
<tr><td>$</td><td>Ende einer Zeile</td></tr>
<tr><td>()</td><td>Einkapselung</td></tr>
<tr><td>[]</td><td>Ein Zeichen in Klammern</td></tr>
<tr><td>|</td><td>ODER</td></tr>
<tr><td>-</td><td>Bereich</td></tr>
<tr><td>\A</td><td>Anfang einer Zeichenfolge</td></tr>
<tr><td>\Z</td><td>Ende einer Zeichenfolge</td></tr>
</table>

Beispiel: Sie wenden die folgenden regulären Ausdrücke an:

<table>
<tr><th>Regulärer Ausdruck</th><th>Ergebnis</th></tr>
<tr><td>(hallo)?</td><td>Enthält entweder „hallo“ oder enthält „hallo“ nicht</td></tr>
<tr><td>(a|b|c)</td><td>a ODER b ODER c</td></tr>
<tr><td>[a-cp]</td><td>a ODER b ODER c ODER p</td></tr>
<tr><td>welt$</td><td>Endet mit „welt“, gefolgt von nichts anderem</td></tr>
</table>

Tabelle 1-5. Lookahead-Operatoren

Regulärer Ausdruck	Beschreibung
?=	Positiver Lookahead (enthält nicht)
?!=	Negativer Lookahead (enthält nicht)

Beispiel: Sie wenden die folgenden regulären Ausdrücke an:

Regulärer Ausdruck	Ergebnis
is (?=\w+)\w{2} primary	is FT primary? Falsch
opid=(?!WFU-1fecf8f9)\S+	WFU-3c9bb994

Tabelle 1-6. Weitere Beispiele für reguläre Ausdrücke

Regulärer Ausdruck	Beschreibung
[xyz]	x, y oder z
(info|warnung|fehler)	Info, Warnung oder Fehler
[a-z]	Ein Kleinbuchstabe
[^a-z]	Kein Kleinbuchstabe
[a-z]+	Ein oder mehrere Kleinbuchstaben
[a-z]*	Null oder mehr Kleinbuchstaben
[a-z]?	Null oder ein Kleinbuchstabe
[a-z] {3}	Genau drei Kleinbuchstaben
[\d]	Eine Ziffer
\d+$	Eine oder mehrere Ziffern, gefolgt vom Ende der Meldung
[0-5]	Eine Zahl von 0 bis 5
\w	Ein Wortzeichen (Buchstabe, Ziffer oder Unterstrich)
\s	Leerzeichen
\S	Ein beliebiges Zeichen außer Leerzeichen
[a-zA-Z0-9]+	Ein oder mehrere alphanumerische Zeichen
([a-z] {2,} [0-9] {3,5})	Zwei oder mehr Buchstaben, gefolgt von drei bis fünf Zahlen

Analysieren von Protokollen mit dem Diagramm „Interaktive Analyse“

Mit dem Diagramm oben auf der Seite **Interaktive Analyse** können Sie visuelle Analysen an den Ergebnissen Ihrer Abfrage ausführen.

Diagramme stellen grafische Snapshots von Protokollsuchabfragen dar. Mit den Dropdown-Menüs unter dem Diagramm können Sie den Diagrammtyp ändern.

Mit dem ersten Dropdown-Menü auf der linken Seite können Sie die Aggregationsebene des Diagramms steuern. Die Funktion **Zähler** ist standardmäßig gewählt.

Zusammenfassungsfunktionen

Log Insight enthält diverse Zusammenfassungsfunktionen.

Typ	Feld	Beschreibung
Zähler	Nur Ereignisse	Erstellt ein Diagramm mit der Anzahl der Ereignisse für eine bestimmte Abfrage.
Anzahl eindeutiger Werte	Jedes Feld	Erstellt ein Diagramm mit der Anzahl eindeutiger Werte für ein Feld.
Mindestwert	Nur numerische Felder	Erstellt ein Diagramm vom Minimalwert für ein Feld.
Maximalwert	Nur numerische Felder	Erstellt ein Diagramm vom Maximalwert für ein Feld.
Durchschnitt	Nur numerische Felder	Erstellt ein Diagramm vom Durchschnittswert für ein Feld.

Typ	Feld	Beschreibung
Std.-Abw.	Nur numerische Felder	Erstellt ein Diagramm von der Standardabweichung für die Werte eines Felds.
Summe	Nur numerische Felder	Erstellt ein Diagramm mit der Summe der Werte für ein Feld.
Varianz	Nur numerische Felder	Erstellt ein Diagramm mit der Varianz für die Werte eines Felds.

Mit dem zweiten Dropdown-Menü unterhalb des Diagramms können Sie Abfrageergebnisse nach bestimmten Feldwerten gruppieren, anstatt sie in Zeitreihen darzustellen, oder zusätzlich zu der Darstellung in Zeitreihen.

Für die Anzeige der Anzahl der Ereignisse für ein Feld, z. B. die Anzahl der Ereignisse pro Host, deaktivieren Sie beispielsweise das Kontrollkästchen **Zeitserie** und aktivieren Sie das Kontrollkästchen für das betreffende Feld.

Für die Anzeige eines Stapelbalkendiagramms für ein Feld mit Gruppierungen im Zeitverlauf aktivieren Sie sowohl das Kontrollkästchen **Zeitserie** als auch das Kontrollkästchen für das betreffende Feld.

Diagrammtypen

Sie können verschiedene Diagrammtypen auswählen, um die Darstellungsmethode der Daten auf der Seite „Interaktive Analyse“ zu ändern.

Welche Zusammenfassungsfunktionen, bzw. ob die Verwendung von Zeitreihen und die Gruppierung nach Feldern erforderlich sind, hängt vom jeweiligen Diagrammtyp ab.

Diagrammtyp	Zusammenfassungsfunktion	Zeitreihe erforderlich	Gruppierung nach Feld erforderlich
Spalte	Alle	Zeitserie	Nicht verfügbar
Zeile	Alle	Zeitserie	Nicht verfügbar
Bereich	Alle	Zeitserie	Nicht verfügbar
Balken	Alle	Nicht-Zeitserie	Mindestens ein Feld
Kreis	Zähler oder Anzahl eindeutiger Werte	Nicht-Zeitserie	Mindestens ein Feld
Blase	Alle	Nicht-Zeitserie	Zwei Felder

Arbeiten mit Protokolldiagrammen

Sie können die Darstellung von Diagrammen auf der Registerkarte **Interaktive Analyse** ändern, Diagramme zu Ihren benutzerdefinierten Dashboards hinzufügen und Dashboard-Diagramme verwalten.

Aufgabe	Vorgehensweise
Ändern des Zeitraums für ein Diagramm	Auf der Registerkarte **Interaktive Analyse** können Sie mit dem Dropdown-Menü links von der Schaltfläche **Suchen** zur Anzeige eines anderen Zeitraums im Diagramm wechseln.
Ändern der Granularität für ein Diagramm	Auf der Registerkarte **Interaktive Analyse** können Sie mit den Schaltflächen oben rechts zwischen verschiedenen Zeiträumen für jeden im Diagramm dargestellten Punkt wechseln. Welche Zeiträume verfügbar sind, hängt von dem für die Abfrage angegebenen Zeitraum ab.
Laden eines Dashboard-Diagramms auf der Registerkarte **Interaktive Analyse**	Suchen Sie auf der Registerkarte **Dashboards** das Diagramm und klicken Sie auf das Symbol **In 'Interaktive Analyse' öffnen** . Als Zeitraum ist der aktuelle Zeitraum des Dashboards eingestellt. Sie können den Zeitraum bei Bedarf ändern.

Aufgabe	Vorgehensweise
Speichern eines Diagramms in Ihrem benutzerdefinierten Dashboard	1 Klicken Sie oben links auf der Registerkarte **Interaktive Analyse** auf **Zum Dashboard hinzufügen**. Wählen Sie alternativ im Menü rechts neben der Schaltfläche **Suchen** die Option **Aktuelle Abfrage zum Dashboard hinzufügen**. 2 Geben Sie einen Namen ein, wählen Sie das Ziel-Dashboard aus dem Dropdown-Menü aus, wählen Sie den Widget-Typ aus, fügen Sie die Informationen über das Widget hinzu und klicken Sie auf **Hinzufügen**.
Speichern einer Abfrage in Ihrem benutzerdefinierten Dashboard	1 Klicken Sie auf **Aktuelle Anfrage zu Dashboard hinzufügen** neben der Schaltfläche **Suchen**. 2 Geben Sie einen Namen ein, wählen Sie das Ziel-Dashboard aus dem Dropdown-Menü aus, stellen Sie sicher, dass als Widget-Typ **Diagramm** eingestellt ist, und klicken Sie auf **Hinzufügen**.
Speichern einer Abfrage als Feldtabelle in Ihrem benutzerdefinierten Dashboard	1 Klicken Sie auf **Aktuelle Anfrage zu Dashboard hinzufügen** neben der Schaltfläche **Suchen**. 2 Geben Sie einen Namen ein, wählen Sie das Ziel-Dashboard aus dem Dropdown-Menü aus, stellen Sie sicher, dass als Widget-Typ **Feldtabelle** eingestellt ist, und klicken Sie auf **Hinzufügen**.
Löschen eines Widgets aus Ihrem benutzerdefinierten Dashboard	1 Wählen Sie auf der Registerkarte **Dashboards** das benutzerdefinierte Dashboard aus, das das Widget enthält, das Sie löschen möchten. 2 Klicken Sie oben rechts im Widget auf das Symbol **Andere Aktionen**, und wählen Sie **Löschen**. 3 Klicken Sie im Dialogfeld Widget löschen zur Bestätigung auf **Löschen**.

Ändern des Diagrammtyps für das Diagramm „Interaktive Analyse“

Sie können die Zusammenfassung und Gruppierung der im Diagramm angezeigten Abfrageergebnisse ändern, um Protokollereignisse grafisch zu analysieren.

Die Anzahl der Dropdown-Menüs, die Sie unter dem Diagramm sehen, hängt von der ausgewählten Zusammenfassungsfunktion ab.

Voraussetzungen

Vergewissern Sie sich, dass Sie bei der Web-Benutzeroberfläche von Log Insight angemeldet sind. Das URL-Format lautet https://*log_insight-host*, wobei *log_insight-host* die IP-Adresse oder der Hostname der virtuellen Log Insight-Appliance ist.

Vorgehensweise

1 Mit den Dropdown-Menüs unter dem Diagramm „Interaktive Analyse“ können Sie die Zusammenfassungsfunktion und den Gruppierungstyp ändern.

   - Aktivieren Sie das Kontrollkästchen **Zeitserie**, um die Anzahl der Ereignisse im Zeitraum anzuzeigen.
   - Wenn Sie nur Ereigniswerte anzeigen möchten, aktivieren Sie das Kontrollkästchen **Nicht-Zeitserie** und wählen Sie mindestens ein Feld aus.

2 Klicken Sie auf **Aktualisieren**.

Beispiel: Zusammenfassung und Gruppierung im Diagramm „Interaktive Analyse“

Die folgende Tabelle enthält Beispiele zur Veranschaulichung der Zusammenfassung und Gruppierung in Log Insight-Diagrammen.

Tabelle 1-7. Beispiel für die Zusammenfassung und Gruppierung im Diagramm „Interaktive Analyse“

Auswahl im ersten Dropdown-Menü	Auswahl im zweiten Dropdown-Menü	Auswahl der Zeitserie	Anzeigetext auf dem Bildschirm	Ergebnis
Zähler	**Zeitserie**	**Zeitserie**	**Anzahl** der Ereignisse **im Zeitraum**	Das Diagramm wird als Balkendiagramm mit der Anzahl der Ereignisse für die aktuelle Abfrage im Zeitraum angezeigt.
Durchschnitt	**vmw_op_latency (VMware – vSphere)**	**Zeitserie**	**Durchschnitt** von **vmw_op_latency (VMware - vSphere) im Zeitraum**	Das Diagramm wird als Liniendiagramm mit dem Durchschnittswert der Latenz der Vorgänge im Zeitraum angezeigt.
Zähler	**vmw_esx_problem** HINWEIS Das Feld vmw_esx_problem wird standardmäßig nicht angezeigt. Sie müssen das Feld vmw_esx_problem extrahieren und die Abfrage speichern, damit vmw_esx_problem im Dropdown-Menü angezeigt wird.	**Nicht-Zeitserie**	**Anzahl** der Ereignisse, **gruppiert nach vmw_esx_problem**	Das Diagramm wird als Balkendiagramm mit der Anzahl der Ereignisse, die das Feld vmw_esx_problem enthalten, angezeigt.
Zähler	**Zeitserie**, **vmw_esx_problem**	**Zeitserie**	**Anzahl** der Ereignisse **im Zeitraum, gruppiert nach vmw_esx_problem**	Das Diagramm wird als Stapelbalkendiagramm angezeigt, wobei die Balken nach vmw_esx_problem im Zeitraum gruppiert sind.

Dynamische Feldextraktion

In einer großen Umgebung mit zahlreichen Protokollereignissen können Sie die für Sie wichtigen Datenfelder nicht immer auffinden.

Log Insight enthält die Laufzeit-Feldextraktion zur Behebung dieses Problems. Durch Angabe eines regulären Ausdrucks können Sie jedes Feld dynamisch aus den Daten extrahieren. Weitere Informationen hierzu finden Sie unter „Beispiele für reguläre Ausdrücke“, auf Seite 17.

HINWEIS Allgemeine Abfragen sind unter Umständen sehr langsam. Wenn Sie beispielsweise versuchen, ein Feld mit dem Ausdruck `\(\d+\)` zu extrahieren, gibt die Abfrage alle Protokollereignisse aus, die Zahlen in Klammern enthalten. Stellen Sie sicher, dass Ihre Abfragen möglichst viel Textkontext enthalten. Eine bessere Feldextraktionsabfrage wäre beispielsweise `Event for vm\(\d+\)`.

Mithilfe der extrahierten Felder können Sie die Liste der Protokollereignisse durchsuchen und filtern, oder Sie können Ereignisse im Diagramm „Interaktive Analyse“ zusammenfassen.

Extrahieren von Feldern mit der Direktextraktion

Anstatt Kontextwerte für die dynamische Extraktion von Feldern einzugeben, können Sie die Direktextraktionsfunktion verwenden.

Bei der Direktextraktion werden alle Kontextwerte, die dem in einem Protokollereignis ausgewählten Feld entsprechen, automatisch angegeben.

HINWEIS Die Direktextraktionsoption ist nur auf der Registerkarte „Ereignisse“ verfügbar.

Voraussetzungen

Vergewissern Sie sich, dass Sie bei der Web-Benutzeroberfläche von Log Insight angemeldet sind. Das URL-Format lautet https://*log_insight-host*, wobei *log_insight-host* die IP-Adresse oder der Hostname der virtuellen Log Insight-Appliance ist.

Vorgehensweise

1 Rufen Sie die Registerkarte **Interaktive Analyse** auf.

2 Markieren Sie in der Liste der Protokollereignisse den Text, der für das Feld steht, das Sie extrahieren möchten.

   Über der Reihe der Feldnamen, die in dem betreffenden Ereignis vorkommen, wird an Aktionsmenü angezeigt.

3 Klicken Sie auf **Feld extrahieren**.

   Die Vor- und Nachkontextwerte im Bereich „Felder“ werden automatisch mit dem Kontext befüllt, der zum Extrahieren des markierten Felds erforderlich ist.

4 (Optional) Ändern Sie den regulären Ausdruck des extrahierten Werts im Fensterbereich „Felder“.

5 (Optional) Ändern Sie die regulären Ausdrücke für den Vor- und Nachkontext im Fensterbereich „Felder“.

6 (Optional) Klicken Sie auf **Zusätzlichen Kontext hinzufügen**, um weitere Schlüsselwörter und Filter hinzuzufügen.

   Sie können ein oder mehrere Schlüsselwörter hinzufügen und ein einzelnes statisches Feld als einen Filter verwenden.

7 Wenn Sie als Administrator angemeldet sind, wählen Sie aus, welche Benutzer über das Dropdown-Menü auf das Feld zugreifen können.

Option	Beschreibung
Alle Benutzer	Allen Benutzern wird das Feld in ihren Ereignissen und im Dropdown-Menü für den Filter angezeigt.
Nur ich	Nur dem Ersteller des Felds wird das Feld in seinen Ereignissen und im Dropdown-Menü für den Filter angezeigt.

8 Klicken Sie auf **Speichern**.

Weiter

Mithilfe des extrahierten Felds können Sie die Liste der Protokollereignisse suchen und filtern, oder Sie können Ereignisse im Diagramm „Interaktive Analyse“ zusammenfassen.

Sie können die gespeicherten Felddefinitionen bearbeiten oder löschen, wenn Sie sie nicht mehr benötigen.

Bearbeiten eines extrahierten Felds

Sie können die Definitionen von extrahierten Feldern bearbeiten.

Log Insight erstellt Kopien der Felder, die Sie beim Erstellen von Diagrammen, Abfragen oder Warnungen verwenden. Wenn Sie eine Felddefinition bearbeiten, werden alle Diagramme, Abfragen und Warnungen, die das bearbeitete Feld verwenden, mit der neuen Definition aktualisiert.

Normale Benutzer können nur ihre eigenen Inhalte bearbeiten. Admin-Benutzer können ihre eigenen Inhalte und ihre freigegebenen Inhalte duplizieren.

Felder in Inhaltspaketen sind schreibgeschützt.

Voraussetzungen

Vergewissern Sie sich, dass Sie bei der Web-Benutzeroberfläche von Log Insight angemeldet sind. Das URL-Format lautet https://*log_insight-host*, wobei *log_insight-host* die IP-Adresse oder der Hostname der virtuellen Log Insight-Appliance ist.

Vorgehensweise

1 Rufen Sie die Registerkarte **Interaktive Analyse** auf.

2 Klicken Sie oben im Fensterbereich „Felder“ auf **Extrahierte Felder verwalten**. zu bearbeiten, und wählen Sie ein extrahiertes Feld aus der Liste aus.

3 Bearbeiten Sie die Werte und klicken Sie auf **Aktualisieren**.

   In einem Dialogfeld wird eine Liste der Inhalte angezeigt, die von dem aktualisierten Feld betroffen sind. Wenn das Feld für mehrere Benutzer freigegeben ist, wird im Dialogfeld auch eine Liste der betroffenen Benutzer angezeigt.

4 Klicken Sie auf **Aktualisieren**, um Ihre Änderungen zu bestätigen.

Log Insight aktualisiert alle Abfragen, Warnungen und Diagramme, die das bearbeitete Feld verwenden.

Duplizieren eines extrahierten Felds

Sie können ein extrahiertes Feld duplizieren.

Verwenden Sie die Option „Duplizieren“, wenn Sie mehr als ein Feld von einem Ereignis extrahieren möchten und beide Felder in ähnlichem Kontext erscheinen. Nachdem Sie ein Feld extrahiert und gespeichert haben, öffnen Sie die extrahierte Felddefinition und verwenden Sie die Option „Duplizieren“. Das duplizierte Feld hat genau dieselbe Definition wie das extrahierte Originalfeld. Sie können die Definition des duplizierten Felds für die Übereinstimmung mit einem anderen Wert in dem Ereignis von Interesse bearbeiten.

Normale Benutzer können nur ihre eigenen Inhalte duplizieren. Admin-Benutzer können ihre eigenen Inhalte und ihre freigegebenen Inhalte duplizieren.

Voraussetzungen

Vergewissern Sie sich, dass Sie bei der Web-Benutzeroberfläche von Log Insight angemeldet sind. Das URL-Format lautet https://*log_insight-host*, wobei *log_insight-host* die IP-Adresse oder der Hostname der virtuellen Log Insight-Appliance ist.

Vorgehensweise

1 Rufen Sie die Registerkarte **Interaktive Analyse** auf.

2 Klicken Sie oben im Fensterbereich „Felder“ auf **Extrahierte Felder verwalten**. zu bearbeiten, und wählen Sie ein extrahiertes Feld aus der Liste aus.

3 Klicken Sie auf **Duplizieren**, um eine Kopie des Felds zu erstellen.

4 (Optional) Ändern Sie den regulären Ausdruck des extrahierten Werts im Fensterbereich „Felder“.

5 (Optional) Ändern Sie die regulären Ausdrücke für den Vor- und Nachkontext im Fensterbereich „Felder“.

6 (Optional) Klicken Sie auf **Zusätzlichen Kontext hinzufügen**, um weitere Schlüsselwörter und Filter hinzuzufügen.

   Sie können ein oder mehrere Schlüsselwörter hinzufügen und ein einzelnes statisches Feld als einen Filter verwenden.

7 Wenn Sie als Administrator angemeldet sind, wählen Sie aus, welche Benutzer über das Dropdown-Menü auf das Feld zugreifen können.

Option	Beschreibung
Alle Benutzer	Allen Benutzern wird das Feld in ihren Ereignissen und im Dropdown-Menü für den Filter angezeigt.
Nur ich	Nur dem Ersteller des Felds wird das Feld in seinen Ereignissen und im Dropdown-Menü für den Filter angezeigt.

8 Klicken Sie auf **Speichern**.

Weiter

Mithilfe des extrahierten Felds können Sie die Liste der Protokollereignisse suchen und filtern, oder Sie können Ereignisse im Diagramm „Interaktive Analyse“ zusammenfassen.

Sie können die gespeicherten Felddefinitionen bearbeiten oder löschen, wenn Sie sie nicht mehr benötigen.

Löschen eines extrahierten Felds

Sie können nicht mehr benötigte extrahierte Felder löschen.

Log Insight erstellt Kopien der Felder, die Sie beim Erstellen von Widgets, Abfragen oder Warnungen verwenden. Wenn Sie ein Feld löschen, das in Widgets, Abfragen oder Warnungen verwendet wird, erstellt Log Insight eine temporäre Kopie des gelöschten Felds für jedes Widget, jede Abfrage oder jede Warnung, das bzw. die das Feld verwendet.

Sie können nur Felder mit dem Symbol **Dieses Feld bearbeiten** neben dem Namen löschen. Normale Benutzer können nur ihre eigenen Inhalte löschen. Admin-Benutzer können ihre eigenen Inhalte und ihre freigegebenen Inhalte löschen.

Felder in Inhaltspaketen sind schreibgeschützt.

Voraussetzungen

Vergewissern Sie sich, dass Sie bei der Web-Benutzeroberfläche von Log Insight angemeldet sind. Das URL-Format lautet https://*log_insight-host*, wobei *log_insight-host* die IP-Adresse oder der Hostname der virtuellen Log Insight-Appliance ist.

Vorgehensweise

1 Rufen Sie die Registerkarte **Interaktive Analyse** auf.

2 Klicken Sie oben im Fensterbereich „Felder“ auf **Extrahierte Felder verwalten** zu bearbeiten, und wählen Sie ein extrahiertes Feld aus der Liste aus.

3 Klicken Sie auf ✖.

   In einem Dialogfeld wird eine Liste der Inhalte angezeigt, die das Feld verwenden, das Sie löschen möchten. Wenn Sie Admin-Benutzer sind und das Feld für mehrere Benutzer freigegeben ist, wird im Dialogfeld auch eine Liste der betroffenen Benutzer angezeigt.

4 Klicken Sie zur Bestätigung auf **Löschen**.

Wenn ein gelöschtes Feld in vorhandenen Abfragen verwendet wird, erstellt Log Insight eine temporäre Kopie des Felds und zeigt diese an, wenn Sie eine Abfrage laden, die das gelöschte Feld verwendet.

Wenn Sie Inhalte exportieren, die temporäre Felder enthalten, erstellt Log Insight die Felder zur Vermeidung von temporären Feldern in dem exportierten Inhaltspaket.

Verwalten von Suchabfragen

Sie können Abfrageergebnisse exportieren, Ihre Abfragen für andere Benutzer freigeben und vorhandene Abfragen speichern, löschen, umbenennen und laden.

Speichern einer Abfrage in Log Insight

Sie können Ihre aktuelle Abfrage und den Zeitraum in Log Insight speichern, um sie später anzusehen. Gespeicherte Abfragen können nur von der Seite **Interaktive Analyse** geladen werden.

Voraussetzungen

Vergewissern Sie sich, dass Sie bei der Web-Benutzeroberfläche von Log Insight angemeldet sind. Das URL-Format lautet https://*log_insight-host*, wobei *log_insight-host* die IP-Adresse oder der Hostname der virtuellen Log Insight-Appliance ist.

Vorgehensweise

1 Führen Sie auf der Registerkarte **Interaktive Analyse** die Abfrage aus, die Sie speichern möchten.

2 Klicken Sie auf das Symbol **Aktuelle Anfrage zu Favoriten hinzufügen** ☆.

3 Geben Sie einen Namen ein und klicken Sie auf **Speichern**.

   HINWEIS Gespeicherte Abfragen umfassen einen festen Zeitraum und werden nicht aktualisiert. Durch das Speichern einer Abfrage erstellen Sie einen Snapshot von den Protokollmeldungen, die zum Zeitpunkt der Speicherung innerhalb des Zeitraums verfügbar sind.

Die Abfrage wird zur Liste der Abfragefavoriten hinzugefügt.

Alle Benutzer, einschließlich Administratoren, haben eine eigene Liste gespeicherter Abfragen.

Umbenennen einer Abfrage in Log Insight

Sie können den Namen einer Abfrage ändern, die Sie in Log Insight gespeichert haben.

Voraussetzungen

Vergewissern Sie sich, dass Sie bei der Web-Benutzeroberfläche von Log Insight angemeldet sind. Das URL-Format lautet https://*log_insight-host*, wobei *log_insight-host* die IP-Adresse oder der Hostname der virtuellen Log Insight-Appliance ist.

Vorgehensweise

1 Rufen Sie die Registerkarte **Interaktive Analyse** auf.

2 Klicken Sie auf das Symbol „Favoritenabfrage“.

3 Zeigen Sie auf die Abfrage, die Sie umbenennen möchten, und klicken Sie auf das Symbol **Diese gespeicherte Abfrage bearbeiten**.

4 Geben Sie einen neuen Namen ein und klicken Sie auf **Speichern**.

Laden einer Abfrage in Log Insight

Sie können Abfragen aus Inhaltspaketen oder gespeicherten Abfragen laden, um diese auf der Registerkarte **Interaktive Analyse** anzuzeigen.

Gespeicherte Abfragen unterscheiden sich von Dashboard-Elementen. Sie werden nicht auf jedem benutzerdefinierten Dashboard angezeigt. Wenn Sie eine gespeicherte Abfrage anzeigen, müssen Sie sie laden.

Alle Benutzer, einschließlich Administratoren, haben eine eigene Liste gespeicherter Abfragen.

Voraussetzungen

Vergewissern Sie sich, dass Sie bei der Web-Benutzeroberfläche von Log Insight angemeldet sind. Das URL-Format lautet https://*log_insight-host*, wobei *log_insight-host* die IP-Adresse oder der Hostname der virtuellen Log Insight-Appliance ist.

Vorgehensweise

1 Rufen Sie die Registerkarte **Interaktive Analyse** auf.

2 Klicken Sie auf das Symbol „Favoritenabfrage“.

3 Klicken Sie in der Liste „Favoritenabfragen“ auf die Abfrage, die Sie auf der Registerkarte **Interaktive Analyse** anzeigen möchten.

   Die Abfrage wird in die Registerkarte **Interaktive Analyse** geladen. Der Zeitraum der Abfrage wird oberhalb der Ereignisliste angezeigt.

Weiter

Sie können die Abfrage zu einem Dashboard hinzufügen, die Granularität des Diagramms ändern oder weitere Filter auf die Abfrageergebnisse anwenden.

Löschen einer Abfrage aus Log Insight

Sie können gespeicherte Abfragen aus Log Insight löschen.

Voraussetzungen

Vergewissern Sie sich, dass Sie bei der Web-Benutzeroberfläche von Log Insight angemeldet sind. Das URL-Format lautet https://*log_insight-host*, wobei *log_insight-host* die IP-Adresse oder der Hostname der virtuellen Log Insight-Appliance ist.

Vorgehensweise

1 Rufen Sie die Registerkarte **Interaktive Analyse** auf.

2 Wählen Sie im Dropdown-Menü rechts von der Schaltfläche **Suchen** die Option **Warnung laden**.

3 Klicken Sie auf das Symbol „Favoritenabfrage“.

4 Klicken Sie in der Liste „Favoritenabfragen“ auf neben der Abfrage, die Sie löschen möchten.

5 Klicken Sie zur Bestätigung auf **Löschen**.

Freigabe der aktuellen Abfrage

Sie können Ihren Kollegen einen Link zu der aktuellen Abfrage senden.

Voraussetzungen

Vergewissern Sie sich, dass Sie bei der Web-Benutzeroberfläche von Log Insight angemeldet sind. Das URL-Format lautet https://*log_insight-host*, wobei *log_insight-host* die IP-Adresse oder der Hostname der virtuellen Log Insight-Appliance ist.

Vorgehensweise

1. Führen Sie auf der Registerkarte **Interaktive Analyse** die Abfrage aus, die Sie freigeben möchten.
2. Klicken Sie auf und wählen Sie **Anfrage freigeben**.

   Log Insight zeigt die URL zu der Abfrage an.
3. Kopieren Sie die URL und senden Sie sie an die Person, für die Sie die Abfrage freigeben möchten.

Exportieren der aktuellen Abfrage

Sie können die Ergebnisse einer Protokollabfrage exportieren, um sie für andere Systeme freizugeben oder an Ihren Support-Ansprechpartner weiterzuleiten.

Voraussetzungen

Vergewissern Sie sich, dass Sie bei der Web-Benutzeroberfläche von Log Insight angemeldet sind. Das URL-Format lautet https://*log_insight-host*, wobei *log_insight-host* die IP-Adresse oder der Hostname der virtuellen Log Insight-Appliance ist.

Vorgehensweise

1. Führen Sie auf der Registerkarte **Interaktive Analyse** die Abfrage aus, die Sie exportieren möchten.
2. Klicken Sie auf und wählen Sie **Ereignisergebnisse exportieren**.
3. Wählen Sie das Format aus, in dem die Abfrage gespeichert werden soll, und klicken Sie auf **Exportieren**.

Option	Beschreibung
Rohereignisse	Wählen Sie diese Option, um die Ergebnisse im TXT-Format zu speichern.
JSON	Wählen Sie diese Option, um die Ergebnisse im JSON-Format zu speichern.
XML	Wählen Sie diese Option, um die Ergebnisse im XML-Format zu speichern.

Arbeiten mit Dashboards

Dashboards in Log Insight sind Sammlungen von Diagramm-, Feldtabellen- und Abfragelisten-Widgets.

Benutzerdefinierte Dashboards

Benutzerdefinierte Dashboards werden von Benutzern der aktuellen Instanz von Log Insight erstellt. Benutzerdefinierte Dashboards sind in zwei Kategorien organisiert: eigene Dashboards und freigegebene Dashboards. Freigegebene Dashboards sind für alle Benutzer der Log Insight-Instanz sichtbar.

Eigene Dashboards sind benutzerspezifisch.

Normale Benutzer können nur die Dashboards im Bereich „Meine Dashboards“ bearbeiten.

Admin-Benutzer können die Dashboards im Bereich „Meine Dashboards“ und die von ihnen erstellten Dashboards im Bereich „Freigegebene Dashboards“ bearbeiten.

Inhaltspaket-Dashboards

Inhaltspaket-Dashboards werden mit Inhaltspaketen importiert und sind für alle Benutzer der Log Insight-Instanz sichtbar.

HINWEIS Inhaltspaket-Dashboards sind schreibgeschützt. Sie lassen sich weder löschen noch umbenennen. Sie können Inhaltspaket-Dashboards jedoch auf Ihr benutzerdefiniertes Dashboard klonen. Sie können ganze Dashboards oder einzelne Widgets klonen.

Sie können die Dashboards anzeigen, die in Ihrer Log Insight-Instanz verfügbar sind. Klicken Sie hierzu oben links in der Log Insight-Benutzeroberfläche auf **Dashboards** . Mit dem Dropdown-Menü oben links können Sie zwischen Dashboard-Kategorien wechseln.

Um die Inhalte eines Dashboards anzuzeigen, klicken Sie auf den Dashboard-Namen links in der Liste.

Verwalten von Dashboards

Sie können Dashboards in Ihrem Bereich „Benutzerdefinierte Dashboards“ hinzufügen, bearbeiten und löschen.

Inhaltspaket-Dashboards können nicht bearbeitet werden, aber Sie können diese Dashboards in Ihrem Bereich „Benutzerdefinierte Dashboards“ klonen und die Klone bearbeiten.

WICHTIG Log Insight führt keine Überprüfungen auf doppelte Namen der Dashboards, Abfragen und Warnungen aus, die Sie speichern oder klonen. Der Anzeigename ist kein eindeutiger Bezeichner, wenn Log Insight Abfragen speichert. Daher können Sie mehrere Diagramme, Warnungen und Dashboards mit demselben Namen speichern. Damit die Daten leicht abrufbar sind, sollten Sie beim Speichern von Diagrammen, Warnungen oder Dashboards dieselben Namen nicht doppelt verwenden.

Tabelle 1-8. Arbeiten mit benutzerdefinierten Dashboards

Aufgabe	Vorgehensweise
Erstellen eines neuen benutzerdefinierten Dashboards	Wählen Sie auf der Registerkarte **Dashboards** die Option **Meine Dashboards** und klicken Sie unten links auf **Neues Dashboard**.
Bearbeiten des Namens eines benutzerdefinierten Dashboards	Bewegen Sie auf der Registerkarte **Dashboards** den Mauszeiger über den Dashboard-Namen, klicken Sie auf das Menüsymbol und wählen Sie **Umbenennen**. Geben Sie einen neuen Namen ein und klicken Sie auf **Speichern**.
Löschen eines benutzerdefinierten Dashboards	Bewegen Sie auf der Registerkarte **Dashboards** den Mauszeiger über den Dashboard-Namen, klicken Sie auf das Menüsymbol und wählen Sie **Löschen**. Wählen Sie im Bestätigungsdialogfeld **Löschen**.
Klonen eines Dashboards aus einem Inhaltspaket in Ihrem benutzerdefinierten Dashboard	1 Wählen Sie auf der Registerkarte **Dashboards** ein Inhaltspaket aus und bewegen Sie den Mauszeiger über das Dashboard, das Sie klonen möchten. 2 Klicken Sie auf das Menüsymbol und wählen Sie im Dropdown-Menü **Klonen**. 3 Geben Sie einen Namen ein und klicken Sie auf **Speichern**. Wenn Sie Admin-Benutzerstatus haben, können Sie Ihr Dashboard wahlweise für andere Benutzer freigeben.

Tabelle 1-8. Arbeiten mit benutzerdefinierten Dashboards (Fortsetzung)

Aufgabe	Vorgehensweise
Hinzufügen eines Diagramm-Widgets zu einem Dashboard	1 Klicken Sie oben links auf der Registerkarte **Interaktive Analyse** auf **Zum Dashboard hinzufügen**. Wählen Sie alternativ im Menü rechts neben der Schaltfläche **Suchen** die Option **Aktuelle Abfrage zum Dashboard hinzufügen**. 2 Geben Sie einen Namen ein, wählen Sie das Ziel-Dashboard aus dem Dropdown-Menü aus, wählen Sie den Widget-Typ aus, fügen Sie die Informationen über das Widget hinzu und klicken Sie auf **Hinzufügen**.
Hinzufügen eines Abfragelisten-Widgets zum Dashboard	Weitere Informationen hierzu finden Sie unter „Hinzufügen eines Abfragelisten-Widgets zum Dashboard“, auf Seite 30.
Hinzufügen einer Abfrage zu einem Abfragelisten-Widget in einem Dashboard	Weitere Informationen hierzu finden Sie unter „Hinzufügen einer Abfrage zu einem Abfragelisten-Widget in einem Dashboard“, auf Seite 31.
Hinzufügen einer Abfrage zu einem Feldtabellen-Widget in einem Dashboard	Siehe „Hinzufügen eines Feldtabellen-Widgets zu einem Dashboard“, auf Seite 31.
Löschen eines Widgets aus einem Dashboard	1 Wählen Sie auf der Registerkarte **Dashboards** das benutzerdefinierte Dashboard aus, das das Widget enthält, das Sie löschen möchten. 2 Klicken Sie oben rechts im Widget auf das Symbol **Andere Aktionen**, und wählen Sie **Löschen**. 3 Klicken Sie im Dialogfeld „Widget löschen“ zur Bestätigung auf **Löschen**.

Hinzufügen eines Abfragelisten-Widgets zum Dashboard

Durch das Erstellen von Abfragelisten-Widgets können Sie Listen von Suchabfragen in Ihren benutzerdefinierten Dashboards speichern.

Voraussetzungen

Vergewissern Sie sich, dass Sie bei der Web-Benutzeroberfläche von Log Insight angemeldet sind. Das URL-Format lautet https://*log_insight-host*, wobei *log_insight-host* die IP-Adresse oder der Hostname der virtuellen Log Insight-Appliance ist.

Vorgehensweise

1 Führen Sie auf der Registerkarte **Interaktive Analyse** die Abfrage aus, die Sie zum Dashboard hinzufügen möchten.

2 Klicken Sie auf das Symbol **Aktuelle Abfrage zu Dashboard hinzufügen** .

3 Wählen Sie im Dropdown-Menü **Dashboard** das Dashboard aus, zu dem Sie die Abfrage hinzufügen möchten.

4 Wählen Sie im Dropdown-Menü **Widget-Typ** die Option **Abfrageliste**.

5 Wählen Sie im Dropdown-Menü **Abfrageliste** die Option **Neue Abfrageliste**, geben Sie einen Namen für die Liste ein und klicken Sie auf **Speichern**.

6 Klicken Sie auf **Hinzufügen**.

Das Abfragelisten-Widget wird auf dem angegebenen Dashboard angezeigt.

Weiter

Sie können Abfragen zu dem erstellten Abfragelisten-Widget hinzufügen. Weitere Informationen hierzu finden Sie unter „Hinzufügen einer Abfrage zu einem Abfragelisten-Widget in einem Dashboard“, auf Seite 31.

Hinzufügen einer Abfrage zu einem Abfragelisten-Widget in einem Dashboard

Abfragelisten-Widgets ermöglichen den Schnellzugriff auf gespeicherte Abfragen über das Dashboard.

Sie können Ihre benutzerdefinierten Abfragelisten-Widgets bearbeiten, um neue Abfragen hinzuzufügen.

Voraussetzungen

Vergewissern Sie sich, dass Sie bei der Web-Benutzeroberfläche von Log Insight angemeldet sind. Das URL-Format lautet https://*log_insight-host*, wobei *log_insight-host* die IP-Adresse oder der Hostname der virtuellen Log Insight-Appliance ist.

Vorgehensweise

1 Führen Sie auf der Registerkarte **Interaktive Analyse** die Abfrage aus, die Sie zum Abfragelisten-Widget hinzufügen möchten.

2 Klicken Sie auf das Symbol **Aktuelle Abfrage zu Dashboard hinzufügen** .

3 Wählen Sie im Dropdown-Menü **Dashboard** das Dashboard aus, das das Abfragelisten-Widget enthält.

4 Wählen Sie im Dropdown-Menü **Widget-Typ** die Option **Abfrageliste**.

5 Wählen Sie im Dropdown-Menü **Abfrageliste** den Namen des Widgets aus, zu dem Sie die Abfrage hinzufügen möchten, und klicken Sie auf **Speichern**.

6 Klicken Sie auf **Hinzufügen**.

Log Insight fügt die Abfrage zu dem ausgewählten Widget hinzu.

HINWEIS Abfragelisten-Widgets verwenden Meldungsabfragen. Wenn Sie dieselbe Meldungsabfrage in einem Diagramm-Widget verwenden und ein Feld als Sortierkriterium auswählen, das in keiner der Meldungen vorhanden ist, zeigt das Diagramm keine Ergebnisse an.

Hinzufügen eines Feldtabellen-Widgets zu einem Dashboard

Feldtabellen-Widgets ermöglichen den Schnellzugriff auf gespeicherte Felder über das Dashboard.

Voraussetzungen

Vergewissern Sie sich, dass Sie bei der Web-Benutzeroberfläche von Log Insight angemeldet sind. Das URL-Format lautet https://*log_insight-host*, wobei *log_insight-host* die IP-Adresse oder der Hostname der virtuellen Log Insight-Appliance ist.

Vorgehensweise

1 Führen Sie auf der Registerkarte **Interaktive Analyse** die Abfrage aus, die Sie zum Feldtabellen-Widget hinzufügen möchten.

2 Klicken Sie auf das Symbol **Aktuelle Abfrage zu Dashboard hinzufügen** .

3 Wählen Sie im Dropdown-Menü **Dashboard** das Dashboard aus, zu dem Sie die Feldtabelle hinzufügen möchten.

4 Wählen Sie im Dropdown-Menü **Widget-Typ** die Option **Feldtabelle**.

5 Wählen Sie die Felder aus, die Sie in die Feldtabelle aufnehmen möchten.

6 Klicken Sie auf **Hinzufügen**.

Das Feldtabellen-Widget wird auf dem angegebenen Dashboard angezeigt.

Filtern mithilfe von Feldwerten aus Diagrammen

Sie können einen Feldwert in einem Diagramm als Filter auf dem Dashboard, das das Diagramm enthält, auf einem anderen Dashboard, das das Feld verwendet, und in der interaktiven Analyse verwenden.

Wenn Sie ein Problem mit einem Feldwert in einem Diagramm sehen, können Sie den Feldwert schnell als Input verwenden und zu einem anderen Dashboard wechseln, das das betreffende Feld verwendet. Wenn kein anderes Dashboard dieses Feld verwendet, können Sie den Feldwert als Filter auf demselben Dashboard verwenden oder in ihn der interaktiven Analyse ausführen.

Voraussetzungen

Vergewissern Sie sich, dass Sie bei der Web-Benutzeroberfläche von Log Insight angemeldet sind. Das URL-Format lautet https://*log_insight-host*, wobei *log_insight-host* die IP-Adresse oder der Hostname der virtuellen Log Insight-Appliance ist.

Vorgehensweise

1 Wählen Sie im Dropdown-Menü **Dashboard** das Dashboard aus, das ein Diagramm-Widget enthält.

2 Bewegen Sie im Diagramm-Widget den Mauszeiger über die Diagrammdaten und zeigen Sie die Feldwerte an, die als Quickinfo angezeigt werden.

3 Klicken Sie auf den Feldwert, den Sie als Filter verwenden möchten.

   Das Menü **Wert als Filter hinzufügen** wird angezeigt.

4 Geben Sie an, ob Sie den Feldwert als Filter verwenden möchten.

Option	Aktion
Interaktive Analyse	Die Seite „Interaktive Analyse“ wird geöffnet. Auf ihr werden die Ergebnisse der Diagrammabfrage angezeigt. Der in Schritt 3 ausgewählte Feldwert wird als Filter verwendet.
Dieses Dashboard	Der in Schritt 3 ausgewählte Feldwert wird als Filter in demselben Dashboard verwendet.
Anderes Dashboard	Der in Schritt 3 ausgewählte Feldwert wird als Filter in einem anderen Dashboard, das das Feld enthält, verwendet.

Arbeiten mit Inhaltspaketen

Inhaltspakete enthalten Dashboards, extrahierte Felder, gespeicherte Abfragen und Warnungen, die sich auf ein bestimmtes Produkt oder auf eine Gruppe von Protokollen beziehen.

Wählen Sie zum Anzeigen der Inhaltspakete, die auf Ihrem System geladen sind, im Dropdown-Menü oben rechts in der Log Insight-Benutzeroberfläche von die Option **Inhaltspakete** aus.

Um die Inhalte eines Inhaltspakets anzuzeigen, klicken Sie auf den Inhaltspaketnamen links in der Liste.

Inhaltspakete

Die Kategorie „Inhaltspakete" enthält importierte Dashboard-Gruppen, extrahierte Felder, Abfragen und Warnungen. Die Inhaltspakete „Allgemein" und „VMware vSphere" werden standardmäßig importiert.

HINWEIS Inhaltspaket-Dashboards sind schreibgeschützt. Sie lassen sich weder löschen noch umbenennen. Sie können Inhaltspaket-Dashboards jedoch auf Ihr benutzerdefiniertes Dashboard klonen. Sie können ganze Dashboards oder einzelne Widgets klonen.

Benutzerdefinierter Inhalt

Die Kategorie „Benutzerdefinierter Inhalt" enthält Dashboards, extrahierte Felder und Abfragen, die in der aktuellen Instanz von Log Insight erstellt wurden. Der Bereich „Meine Inhalte" enthält die benutzerdefinierten Inhalte des Benutzers, der gegenwärtig angemeldet ist. Der Bereich „Freigegebener Inhalt" enthält Inhalte, die für alle Benutzer von Log Insight freigegeben wurden.

Nur Admin-Benutzer können Inhalte für andere Benutzer freigeben. Nur Admin-Benutzer können freigegebene Inhalte verwalten.

HINWEIS Sie können keine Inhalte aus dem Bereich „Benutzerdefinierter Inhalt" deinstallieren. Wenn Sie die gespeicherten Informationen aus dem Bereich „Benutzerdefinierter Inhalt" entfernen möchten, müssen Sie einzelne Elemente löschen, z. B. Dashboards, Abfragen, Warnungen und Felder.

Exportieren eines Inhaltspakets

Sie können Ihre benutzerdefinierten Dashboards, gespeicherten Suchvorgänge, Warnungen und extrahierten Felder als Inhaltspaket exportieren und mit anderen Instanzen von Log Insight oder Benutzern von Log Insight in der Community gemeinsam verwenden.

Inhaltspakete werden als vCenter Log Insight-Inhaltdateien (VLCP) gespeichert.

Alle in den exportierten Abfragen, Diagrammen und Warnungen verwendeten Felder sind im exportierten Inhaltspaket enthalten.

Wenn Sie Inhalte mit temporären Feldern exportieren, werden diese von Log Insight während des Exports im exportierten Inhaltspaket erstellt.

Voraussetzungen

Vergewissern Sie sich, dass Sie bei der Web-Benutzeroberfläche von Log Insightals Benutzer mit der Berechtigung **Admin bearbeiten** angemeldet sind. Das URL-Format lautet https://*log-insight-host*, wobei *log-insight-host* die IP-Adresse oder der Hostname der virtuellen Log Insight-Appliance ist.

Vorgehensweise

1 Wählen Sie im Dropdown-Menü oben rechts **Inhaltspakete**.

2 Klicken Sie auf das Inhaltspaket, das Sie exportieren möchten, und wählen Sie **Exportieren** aus dem im Dropdown-Menü neben dem Namen des Inhaltspakets.

3 (Optional) Wählen Sie den gewünschten Inhalt des Pakets aus.

HINWEIS Felder, die in Dashboards, Abfragen oder Warnungen für den Export ausgewählt sind, können nicht deaktiviert werden.

---

4 Geben Sie in den Textfeldern rechts die Metadaten Ihres Inhaltspakets ein.

Option	Beschreibung
Name	Der Name wird angezeigt, wenn Sie das Paket in eine Instanz von Log Insight importieren. Der Name des Inhaltspakets wird aus dem Textfeld **Name** übernommen. Das empfohlene Format lautet *Anbieter – Produkt*, etwa VMware – vSphere.
Version	Wenn Sie das Inhaltspaket später aktualisieren möchten, geben Sie eine Versionsnummer ein. Log Insight zeigt die Version an, wenn Sie versuchen, ein Inhaltspaket zu installieren, das bereits in der Liste der Inhaltspakete vorhanden ist.
Namespace	Der Namespace ist ein eindeutiger Bezeichner des Inhaltspakets. Verwenden Sie die umgekehrte DNS-Benennung, beispielsweise **`com.firmenname.inhaltspaketsname`**.
Autor	Optional können Sie Ihren Namen oder den Ihrer Firma eingeben.
Website	Optional können Sie einen Link zu einer Website für das Inhaltspaket angeben. Alle Benutzer, die das Inhaltspaket anzeigen, sehen auch diesen Link zur Website.
Beschreibung	Optional können Sie Informationen über den Inhalt und den Zweck des Pakets angeben.
Symbol	Optional können Sie ein Symbol auswählen, das neben dem Namen des Inhaltspakets angezeigt wird. HINWEIS Die Symboldatei muss im Format PNG oder JPG vorliegen und wird auf 144 mal 144 Pixel skaliert.

HINWEIS Diese Daten sind nur dann sichtbar, wenn Sie das Inhaltspaket mithilfe der Option **Als Inhaltspaket installieren** importieren. Diese Informationen werden nicht angezeigt, wenn Sie das Inhaltspaket als benutzerdefinierten Inhalt importieren.

5 Klicken Sie auf **Exportieren**, gehen Sie zum gewünschten Speicherort und klicken Sie auf **Speichern**.

Die exportierte VLCP-Datei wird am ausgewählten Ort gespeichert.

Installieren eines Inhaltspakets aus dem Download-Center für Inhaltspakete

Inhaltspakete können ohne Verlassen der Log Insight-Benutzeroberfläche aus dem Download-Center für Inhaltspakete installiert werden.

Voraussetzungen

- Vergewissern Sie sich, dass Sie bei der Web-Benutzeroberfläche von Log Insight angemeldet sind. Das URL-Format lautet https://*log_insight-host*, wobei *log_insight-host* die IP-Adresse oder der Hostname der virtuellen Log Insight-Appliance ist.
- Stellen Sie sicher, dass Sie als Benutzer mit der Berechtigung **Freigegebenen Inhalt bearbeiten** angemeldet sind.

Vorgehensweise

1 Wählen Sie im Dropdown-Menü oben rechts **Inhaltspakete**.

2 Wählen Sie im Menü links die Option **Download-Center** aus.

3 Wählen Sie das gewünschte Inhaltspaket aus und klicken Sie auf **Installieren**.

Das installierte Inhaltspaket erscheint in der Liste der installierten Inhaltspakete auf der linken Seite.

Aktualisieren eines installierten Inhaltspakets aus dem Download-Center für Inhaltspakete

Sie können die Inhaltspakete, die bereits vom Download-Center für Inhaltspakete installiert wurden, aktualisieren, ohne dazu die Log Insight-Benutzeroberfläche verlassen zu müssen.

Voraussetzungen

- Vergewissern Sie sich, dass Sie bei der Web-Benutzeroberfläche von Log Insight angemeldet sind. Das URL-Format lautet https://*log_insight-host*, wobei *log_insight-host* die IP-Adresse oder der Hostname der virtuellen Log Insight-Appliance ist.
- Stellen Sie sicher, dass Sie als Benutzer mit der Berechtigung **Freigegebenen Inhalt bearbeiten** angemeldet sind.

Vorgehensweise

1 Wählen Sie im Dropdown-Menü oben rechts **Inhaltspakete**.

2 Wählen Sie aus dem Menü links die Option **Updates** aus.

3 Wenn Updates verfügbar sind, wählen Sie das Inhaltspaket, das Sie aktualisieren möchten, und klicken Sie auf **Aktualisieren**.

4 (Optional) Klicken Sie auf **Alle aktualisieren**, um alle verfügbaren Inhaltspaket-Updates anzuwenden.

Das aktualisierte Inhaltspaket wird in der Liste „Installierte Inhaltspakete“ auf der linken Seite angezeigt.

Importieren eines Inhaltspakets

Sie können Inhaltspakete importieren, um benutzerdefinierte Informationen mit anderen Instanzen von Log Insightauszutauschen oder um ein Upgrade Ihrer alten Inhaltspakete auf neuere Versionen durchzuführen.

Sie können nur vCenter Log Insight Content Pack (VLCP)-Dateien importieren.

HINWEIS Wenn Sie eine neue Version eines bereits vorhandenen Inhaltspakets importieren und die neue Version geänderte Felddefinitionen umfasst, werden alle Anfragen, Warnungen und Diagramme, welche auf das geänderte Feld zurückgreifen, aktualisiert, um so die neue Definition widerzuspiegeln. Wenn Felder der aktuellen Version des Inhaltspakets in der neuen von Ihnen importierten Version fehlen, erstellt Log Insight für jede Anfrage, jedes Diagramm bzw. jede Warnung, die auf ein gelöschtes Feld zurückgreift, temporäre Kopien der Felder.

Voraussetzungen

Vergewissern Sie sich, dass Sie bei der Web-Benutzeroberfläche von Log Insightals Benutzer mit der Berechtigung **Admin bearbeiten** angemeldet sind. Das URL-Format lautet https://*log-insight-host*, wobei *log-insight-host* die IP-Adresse oder der Hostname der virtuellen Log Insight-Appliance ist.

Vorgehensweise

1 Wählen Sie im Dropdown-Menü oben rechts **Inhaltspakete**.

2 Klicken Sie in der unteren linken Ecke auf **Inhaltspaket importieren**.

3 Wenn Sie ein Admin-Benutzer sind, wählen Sie das Importverfahren aus.

Option	Beschreibung
Als Inhaltspaket installieren	Der Inhalt wird als schreibgeschütztes Inhaltspaket importiert, das für alle Benutzer der Log Insight-Instanz sichtbar ist. **Hinweis** Inhaltspaket-Dashboards sind schreibgeschützt. Sie lassen sich weder löschen noch umbenennen. Sie können Inhaltspaket-Dashboards jedoch auf Ihr benutzerdefiniertes Dashboard klonen. Sie können ganze Dashboards oder einzelne Widgets klonen.
In „Mein Inhalt" importieren	Der Inhalt wird als benutzerdefinierter Inhalt in Ihren Benutzerspeicherplatz importiert und ist nur für Sie sichtbar. Sie können den importierten Inhalt bearbeiten, ohne ihn zuvor klonen zu müssen. **Hinweis** Inhaltspaket-Metadaten wie Name, Verfasser, Symbol usw. werden in diesem Modus nicht dargestellt. Nachdem das Inhaltspaket in „Mein Inhalt" importiert wurde, kann es als Paket nicht mehr deinstalliert werden. Wenn Sie ein Inhaltspaket aus „Mein Inhalt" deinstallieren möchten, müssen Sie jedes seiner Elemente wie Dashboards, Anfragen, Warnungen und Felder einzeln deinstallieren.

Normale Benutzer können Inhaltspakete nur in ihre eigenen Benutzerspeicherplätze importieren.

4 Navigieren Sie zu dem Inhaltspaket, das Sie importieren möchten, und klicken Sie auf **Öffnen**.

5 Klicken Sie auf **Importieren**.

Wenn Sie die Option „Als benutzerdefinierter Inhalt importieren" ausgewählt haben, wird Ihnen ein Dialogfeld eingeblendet, in dem Sie auswählen können, welche Inhalte Sie importieren möchten.

6 (Optional) Wenn Sie den Inhalt als benutzerdefinierten Inhalt importieren möchten, aktivieren Sie die Kontrollkästchen für die gewünschten Elemente und klicken Sie dann erneut auf **Importieren**.

Hinweis Felder, die in importierten Anfragen, Diagrammen und Warnungen verwendet werden, werden ebenfalls importiert.

Der importierte Inhalt wird in den Inhaltspaketen oder in der Liste „Benutzerdefinierte Inhalte" auf der linken Seite angezeigt.

Hinweis Importierte Warnungen sind standardmäßig deaktiviert. Weitere Informationen hierzu finden Sie unter „Aktivieren einer Warnungsabfrage", auf Seite 54.

Anzeigen von Details zu Inhaltspaketelementen

Sie können die Abfragen, die Dashboards bilden, oder die Definitionen von Feldern, Abfragen und Warnungen direkt von der Ansicht „Inhaltspakete" aus öffnen.

Möglicherweise möchten Sie die Definitionen von Inhaltspaketelementen als Vorlagen für Ihre benutzerdefinierten Definitionen verwenden.

Voraussetzungen

Vergewissern Sie sich, dass Sie bei der Web-Benutzeroberfläche von Log Insight angemeldet sind. Das URL-Format lautet https://*log_insight-host*, wobei *log_insight-host* die IP-Adresse oder der Hostname der virtuellen Log Insight-Appliance ist.

Vorgehensweise

1 Wählen Sie im Dropdown-Menü oben rechts **Inhaltspakete**.

2 Wählen Sie das Inhaltspaket aus, das das Element enthält, das Sie überprüfen möchten.

3 Klicken Sie auf die Schaltfläche, die dem Elementtyp entspricht, den Sie anzeigen möchten.

   Klicken Sie beispielsweise auf **Warnungen**, um alle im Inhaltspaket enthaltenen Warnungen anzuzeigen.

4 Klicken Sie in der Liste der Elemente auf den Namen des Elements, das Sie überprüfen möchten.

Daraufhin wird die Seite Interaktive Analyse geöffnet, und die Warnungsabfrage, die dem ausgewählten Element entspricht, wird angezeigt.

Weiter

Sie können die Abfrage oder Definition des Inhaltspaketelements bearbeiten und in Ihrem benutzerdefinierten Inhalt speichern.

Erstellen von Inhaltspaketen

Jeder Log Insight-Benutzer kann ein Inhaltspaket für die private oder öffentliche Nutzung erstellen.

Inhaltspakete sind unveränderbare oder schreibgeschützte Plug-Ins für Log Insight, die vordefiniertes Wissen zu bestimmten Arten von Ereignissen beinhalten, z. B. Protokollmeldungen. Das Ziel eines Inhaltspakets besteht darin, Kenntnisse über eine bestimmte Ereignisgruppe in einem Format bereitzustellen, das für Administratoren, Techniker, Überwachungsteams und Führungskräfte einfach verständlich ist.

Inhaltspakete enthalten Informationen über den Zustand eines Produkts oder einer Anwendung. Darüber hinaus können Sie mithilfe von Inhaltspaketen nachvollziehen, wie ein Produkt oder eine Anwendung funktioniert.

Die Informationen aus einem Inhaltspaket können Sie anhand der „Dashboards“-Seite oder anhand der „Interaktive Analyse“-Seite in Log Insight speichern. Die Informationen in einem Inhaltspaket enthalten:

- Abfragen: Ein Inhaltspaket enthält in der Regel mindestens drei Abfragediagramm-Widgets für jedes Dashboard, d. h. insgesamt neun Abfragen.
- Felder: Ein Inhaltspaket sollte mindestens zwanzig extrahierte Felder enthalten.
- Zusammenfassungen
- Warnungen: Jedes Inhaltspaket enthält mindestens fünf Warnungen.
- Dashboards: Jedes Inhaltspaket enthält mindestens drei Dashboards.
- Dashboard-Filter - siehe „Suchen und Filtern von Protokollereignissen“, auf Seite 9
- Visualisierungen - siehe „Analysieren von Protokollen mit dem Diagramm „Interaktive Analyse““, auf Seite 19

Standardmäßig wird Log Insight mit dem VMware vSphere-Inhaltspaket geliefert. Bei Bedarf können Sie weitere Inhaltspakete importieren.

Begriffe zu Inhaltspaketen

Der Arbeitsablauf beim Erstellen von Inhaltspaketen basiert auf diversen Grundbegriffen. Sie sollten sich mit diesen vertraut machen, damit Sie Inhaltspakete effektiv erstellen und pflegen können.

Instanz

Nur Log Insight-Administratoren können eine Inhaltspaketdatei als Inhaltspaket importieren. Wenn ein Inhaltspaket als Inhaltspaket importiert wird, kann es nicht bearbeitet werden.

Alle Benutzer können eine Inhaltspaketdatei in einen Benutzerbereich importieren. Wenn Sie eine Inhaltspaketdatei in einen Benutzerbereich importieren, werden bei dem Vorgang gezielt die Objekte unter „Meine Inhalte“ importiert. Wenn Sie ein Inhaltspaket in einen Benutzerbereich importieren, können Sie die Inhaltspakete in einer Log Insight-Instanz bearbeiten. Wenn Sie ein Inhaltspaket veröffentlichen oder bearbeiten möchten, benötigen Sie ein exportiertes Inhaltspaket.

Benutzer

Inhaltspakete werden teilweise aus den unter „Benutzerdefinierte Dashboards“ gespeicherten Inhalten erstellt. Diese werden auch als Benutzerbereich bezeichnet. Im Einzelnen handelt es sich entweder um „Meine Dashboards“ oder „Freigegebene Dashboards“ auf der Seite „Dashboards“. Objekte aus einem benutzerdefinierten Dashboard können gezielt exportiert werden. Es empfiehlt sich jedoch, dass jedes einzelne Inhaltspaket von einer separaten Benutzerentität in Log Insight erstellt wird, um einen sauberen Benutzerbereich für jedes Inhaltspaket zu gewährleisten.

Informationen zum Erstellen von Benutzern in Log Insight finden Sie im *Administratorhandbuch zu VMware vRealize Log Insight*.

Verwenden Sie für jedes erstellte Inhaltspaket einen eigenen Log Insight-Benutzer als Verfasser des Inhaltspakets.

Ereignisse

Es ist unverzichtbar, relevante Ereignisse zu erfassen, bevor Sie ein Inhaltspaket zu erstellen versuchen, um sicherzustellen, dass ein Inhaltspaket alle relevanten Ereignisse für ein Produkt oder eine Anwendung abdeckt. Eine gängige Möglichkeit zum Erfassen relevanter Ereignisse besteht darin, die Qualitätssicherungs- und Supportteams zu befragen, da diese Teams in der Regel Zugriff auf gängige Ereignisse haben und sich in ihnen auskennen.

Versuche, Ereignisse beim Erstellen eines Inhaltspakets zu generieren, sind zeitaufwändig und Ihnen können dabei wichtige Ereignisse entgehen. Wenn die QS- und Supportteams Ihnen keine Angaben über Ereignisse machen können, können Sie stattdessen Ereignisse simulieren und diese verwenden, wenn die Produkt- oder Anwendungsereignisse bekannt und dokumentiert sind.

Nachdem Sie die entsprechenden Protokolle gesammelt haben, müssen diese in Log Insight aufgenommen werden.

Verfasser

Die Verfasser eines Inhaltspakets müssen über die folgenden Qualifikationen verfügen:

- Erfahrungen im Umgang mit VMware vRealize Log Insight.
- Praxiskenntnisse in der Benutzung des Produkts bzw. der Anwendung.
- Kenntnisse und Fähigkeiten im Generieren optimierter regulärer Ausdrücke.
- Erfahrungen im Debuggen zahlreicher Probleme beim Produkt oder bei der Anwendung mithilfe von Protokollen.
- Support-Hintergrund mit Erfahrungen in einer großen Vielfalt von Problemen.
- Hintergrund als Systemadministrator mit Syslog-Erfahrungen.

Workflow

Beim Erstellen von Inhaltspaketen empfiehlt es sich, auf der Seite „Interaktive Analyse“ zu beginnen und zuerst Abfragen für bestimmte Ereignistypen durchzuführen, z. B. „Fehler“ oder „Warnung“. Sehen Sie sich die Abfrageergebnisse an und analysieren und extrahieren Sie Ereignisse, die je nach Bedarf potenziell für Felder in Frage kommen. Bauen Sie aufgrund Ihrer Kenntnisse über die Arten von Ereignissen und in den Ereignissen vorhandener nützlicher Daten je nach Bedarf die relevanten Abfragen auf und speichern Sie sie. Erstellen und speichern Sie Warnungen für Abfragen, die ein Problem hervorheben, das ein schnelles Ein-

greifen erfordert. Beim Speichern Ihrer Abfragen entfernen Sie diese mithilfe einer Einschränkung aus der Ergebnisliste, damit andere Ereignisse angezeigt werden, die möglicherweise für neue gespeicherte Abfragen von Interesse sind. Nachdem Sie alle relevanten Abfragen gespeichert haben, organisieren Sie diese auf eine logische Weise und zeigen Sie sie auf der Seite „Dashboards“ an.

Abfragen

Abfragen in Log Insight können Ereignisse abrufen und zusammenfassen.

Sie können Abfragen über die Seite „Interaktive Analyse“ erstellen und speichern. Eine Abfrage besteht aus einem oder mehreren der folgenden Elemente:

Schlüsselwörter Vollständige Suche oder Volltextsuche, alphanumerische Suche, Bindestrich- und/oder Unterstrichsuche.

Globs Vollständige Suche oder Volltextsuche, alphanumerische Suche, Bindestrich- und/oder Unterstrichsuche.

Reguläre Ausdrücke Abgleich komplexer Zeichenfolgemuster anhand von regulären Java-Ausdrücken.

Feldvorgänge Anwendung der Suche nach Schlüsselwörtern, regulären Ausdrücken und Mustern auf die extrahierten Felder.

Zusammenfassungen Funktionen, die auf eine oder mehrere Untergruppen der Ergebnisse angewandt werden.

Log Insight unterstützt die folgenden Abfragetypen:

- Meldung. Eine Abfrage, die sich aus Schlüsselwörtern, regulären Ausdrücken und/oder Feldvorgängen zusammensetzt.
- Regulärer Ausdruck oder Feld. Eine Abfrage, die sich aus Schlüsselwörtern und/oder regulären Ausdrücken zusammensetzt.
- Zusammenfassung. Eine Abfrage, die sich aus einer Funktion, einer oder mehreren Gruppierungen und einer beliebigen Zahl an Feldern zusammensetzt.

In Log Insight können Sie benutzerdefinierte Warnungen definieren und diese über geplante Abfragen jeder Art auslösen.

Bewährte Praktiken beim Erstellen von Meldungsabfragen

Grundlagen für das Erstellen von Meldungsabfragen

Sie können Meldungsabfragen über die Suchleiste eingeben oder durch die Eingabe von Einschränkungen.

Die Suchleiste ist eine Möglichkeit, die ausgegebenen Ergebnisse innerhalb der vorhandenen Ereignisse in einer Log Insight-Instanz einzugrenzen. Sie können eine Einschränkung zwar anstelle der Suchleiste verwenden, aber Abfragen, die über die Suchleiste durchgeführt werden, sind oft leichter nachzuvollziehen als Abfragen mit einer gleichwertigen Einschränkung. Daher hat es sich bewährt, nach Möglichkeit die Suchleiste zu verwenden statt einer gleichwertigen Einschränkung.

Mit einer Einschränkung können Sie Abfragen mithilfe eines regulären Ausdrucks, eines Felds, eines logischen ODER-Operators oder einer Kombination aus Suchleisten- und Einschränkungsabfragen erstellen.

Beim Erstellen von Abfragen mithilfe der Suchleiste und Einschränkungen haben sich die folgenden Praktiken bewährt:

- Achten Sie darauf, dass die Abfragen nicht umgebungsspezifisch sind. Öffentliche Inhaltspakete müssen generisch für jede Umgebung sein und dürfen sich daher nicht auf umgebungsspezifische Informationen stützen. Beispiele für umgebungsspezifische Informationen sind Quelle, Hostname und möglicherweise der Betrieb, sofern dieser *local** verwendet.

- Verwenden Sie beim Aufbau einer Abfrage nach Möglichkeit Schlüsselwörter. Wenn Schlüsselwörter nicht ausreichen, verwenden Sie Globs, und wenn Globs nicht ausreichend sind, verwenden Sie reguläre Ausdrücke. Schlüsselwortabfragen sind der am wenigsten ressourcenintensive Abfragetyp. Globs sind eine vereinfachte Form von regulären Ausdrücken. Sie sind die am zweitwenigsten ressourcenintensive Art der Abfrage. Reguläre Ausdrücke sind der ressourcenintensivste Abfragetyp.
- Geben Sie bei der Verwendung von regulären Ausdrücken oder Feldern so viele Schlüsselwörter an wie möglich. Wenn ein regulärer Ausdruck den logischen Operator ODER enthält, beispielsweise *dies|jenes*, sollten Sie keine Schlüsselwörter aufnehmen. Log Insight ist dahingehend optimiert, dass Schlüsselabfragen vor Abfragen mit regulären Ausdrücken ausgeführt werden, um unerwünschte Treffer für reguläre Ausdrücke möglichst weit einzugrenzen.

Feldabfragen

Felder sind eine leistungsstarke Möglichkeit, unstrukturierte Ereignisse mit einer Struktur zu versehen, und ermöglichen die Veränderung textueller und visueller Darstellungen von Daten.Log Insight

Felder gehören zu den wichtigsten Bestandteilen in einem Inhaltspaket, weil sie auf unterschiedliche Weise eingesetzt werden können, z. B. für Zusammenfassungen und Einschränkungen. Mit Zusammenfassungen können Sie Funktionen und Gruppierungen auf Felder anwenden. Mit Beschränkungen können Sie Vorgänge an Feldern ausführen.

Sie müssen die Teile einer Protokollmeldung, die für eine Abfrage oder Zusammenfassung relevant sein können, extrahieren. Felder sind ein Abfragetyp, der auf regulären Ausdrücken basiert. Sie sind hilfreich beim Abgleich komplexer Muster, weil Sie komplizierte reguläre Ausdrücke so nicht kennen, im Gedächtnis behalten oder lernen müssen.

Feldkontextwert	Definition
Regex vor Wert	Nehmen Sie so viele Schlüsselwörter wie möglich auf. Wenn dieses Feld leer ist oder nur Sonderzeichen enthält, muss der Regex nach dem Wert Schlüsselwörter enthalten.
Regex nach Wert	Nehmen Sie so viele Schlüsselwörter wie möglich auf. Wenn dieses Feld leer ist oder nur Sonderzeichen enthält, muss der Regex vor dem Wert Schlüsselwörter enthalten.
Name	Verwenden Sie nur alphanumerische Zeichen. Achten Sie darauf, dass alle Zeichen in Kleinschrift geschrieben sind, und verwenden Sie Unterstriche anstelle von Leerzeichen, weil die Felder dadurch leichter angezeigt werden können. Denken Sie daran, dass Namen für Inhaltspaketfelder und Benutzerfelder identisch sein können, aber Inhaltspaketfelder haben rechts vom Feldnamen einen Namespace in Klammern. Stellen Sie den Inhaltspaketfeldern der Eindeutigkeit halber eine Abkürzung als Präfix voran, z. B. „vmw_“.

Best Practices

Zusätzlich zu den diversen Komponenten, die ein Feld bilden, sollten einige bewährte Praktiken beachtet werden.

- Erstellen Sie nur Felder für reguläre Ausdrucksmuster. Wenn ein Feld mit Schlüsselwortabfragen abgefragt werden kann oder immer nur einen einzelnen Wert ausgibt, sollten Sie Schlüsselwortabfragen anstelle eines vordefinierten Felds verwenden. Wenn ein Feld nur zwei Werte ausgibt, sollten Sie den Aufbau einzelner Abfragen in Betracht ziehen, anstatt ein Feld zu extrahieren. Felder dienen dazu, unstrukturierte Daten mit einer Struktur zu versehen. Außerdem bieten sie eine Möglichkeit, Daten zu bestimmten Teilen eines Ereignisses abzufragen.
- Erstellen Sie nur Felder für reguläre Ausdrucksmuster, die einen Teil der gesamten Ereignisse ausgeben. Felder, die mit den meisten Ereignissen übereinstimmen und/oder eine sehr große Anzahl an Ergebnissen ausgeben, eignen sich nicht besonders gut für die Feldextraktion. Der reguläre Ausdruck muss auf eine große Menge von Ereignissen angewandt werden. Dies führt zu einem ressourcenintensiven Vorgang. Fügen Sie nach Möglichkeit weitere Schlüsselwörter hinzu, um die Zahl der ausgegebenen Ergebnisse einzugrenzen und die Abfrage zu optimieren.

- Wenn ein Feld Schlüsselwörter innerhalb der Syntax eines regulären Ausdrucks enthält, fügen Sie diese Schlüsselwörter als Einschränkung ohne die Syntax des regulären Ausdrucks hinzu. Beispiel: Wenn der Wert oder der Kontext eines Felds Schlüsselwörter innerhalb der Syntax eines regulären Ausdrucks, z. B. *dies|jenes*, enthält, fügen Sie die Schlüsselwörter als Texteinschränkung hinzu, um die Abfrage zu optimieren, z. B. `Text enthält dies, jenes`.

Temporäre Felder

Ein temporäres Feld ist ein Feld, das als Teil einer Abfrage vorhanden ist, das aber nicht global innerhalb einer Log Insight-Instanz oder als Teil eines installierten Inhaltspakets gespeichert wird.

Log Insight reduziert die Möglichkeiten, ein temporäres Feld zu erstellen, durch automatische Aktualisierung der Abfrage, die auf einem in Bearbeitung befindlichen Feld basiert.

HINWEIS Wenn Sie ein Feld löschen, auf dem eine gespeicherte Abfrage basiert, enthält die gespeicherte Abfrage ein temporäres Feld.

Sie können temporäre Felder sehen, wenn Sie eine gespeicherte Abfrage auf der Seite „Interaktive Analyse" ausführen und ein in der gespeicherten Abfrage verwendetes Feld den Namespace „Temporär" rechts neben dem Feldnamen enthält.

Abfragen, die ein oder mehrere Felder enthalten. Für in Log Insight gespeicherte Abfragen wird die Felddefinition, die beim Speichern einer Abfrage verwendet wird, bei der Bearbeitung des Felds ebenfalls bearbeitet. Folgende Feldbearbeitungen sind möglich:

- Ändern des Feldwerts
- Ändern des Regex vor Wert und des Regex nach Feldwert
- Ändern des Feldnamens
- Löschen des Felds

Wenn Sie ein Inhaltspaket exportieren, konvertiert Log Insight alle temporären Felder in Inhaltspaketfelder. Wenn Sie ein temporäres Feld in einem Inhaltspaket sehen, betrachten Sie möglicherweise ein Inhaltspaket aus einer früheren Produktversion, das mit temporären Feldern exportiert wird, oder das Inhaltspaket wird manuell bearbeitet.

Zusammenfassungsabfragen

Mit Log Insight können Sie die visuelle Darstellung von Ereignissen mithilfe von Zusammenfassungsabfragen bearbeiten.

Zusammenfassungsabfragen bestehen aus zwei verschiedenen Attributen

- Funktionen
- Gruppierungen

Für eine Zusammenfassungsabfrage ist eine Funktion und mindestens eine Gruppierung erforderlich. Gruppierungen sind ein wichtiger Bestandteil der Inhaltspakete. Funktionen und Gruppierungen wirken sich auf die Art und Weise aus, wie Diagramme angezeigt werden.

Balkendiagramme

Standardmäßig zeigt das Überblicksdiagramm auf der Seite „Interaktive Analyse" von Log Insight die Anzahl der Ereignisse im Zeitverlauf an. Wenn Sie die Zählfunktion zusammen mit der Zeitreihengruppierung verwenden, erstellt Log Insight ein Säulendiagramm.

Wenn Sie die Zählfunktion zusammen mit einer Einzelfeldgruppierung anstelle einer Zeitreihe verwenden, erstellt Log Insight Balkendiagramme, bei denen die Mengen in absteigender Reihenfolge aufgeführt sind.

Liniendiagramme

Alle Funktionen mit Ausnahme der Zählfunktion sind mathematisch. Sie erfordern ein Feld, auf das Sie die Gleichung anwenden können. Wenn Sie eine mathematische Funktion für ein Feld und eine Gruppierung nach Zeitreihen ausführen, erstellt Log Insight ein Liniendiagramm.

Stapeldiagramme

Standardmäßig zeigt das Überblicksdiagramm auf der Seite „Interaktive Analyse" von Log Insight die Anzahl der Ereignisse im Zeitverlauf an. Wenn Sie ein Feld zu der Zeitreihengruppierung hinzufügen, erstellt Log Insight ein Stapeldiagramm.

Wenn Sie die Gruppierung nach Zeitreihen zusammen mit einem Feld verwenden und eine beliebige Funktion (außer der Zählfunktion) anwenden, erstellt Log Insight ein Stapelliniendiagramm. Stapeldiagramme sind hilfreich bei der Suche nach Anomalien für ein Objekt.

Sie müssen entscheiden, welchen Stapeldiagrammtyp Sie verwenden möchten, je nach der Anzahl der Objekte, die die Zusammenfassungsabfrage vermutlich ausgibt. Bei der Anzeige einer größeren Zahl von Objekten werden mehr Ressourcen zum Analysieren und Anzeigen der Daten benötigt. Außerdem ist die Anzahl der Farben festgelegt und die Unterscheidung zwischen den Objekten kann schwierig werden, je nachdem, wie viele Objekte ausgegeben werden. Generell sind die folgenden Praktiken zu empfehlen:

- Wenn die Anzahl der ausgegebenen Objekte in jedem Balken weniger als 10 beträgt, sind Stapeldiagramme vermutlich sinnvoll.
- Wenn die Anzahl der ausgegebenen Objekte in jedem Balken 10-20 beträgt oder betragen könnte, sind Stapeldiagramme eventuell sinnvoll. Sie müssen sich überlegen, wie das Diagramm in einem Inhaltspaket visuell dargestellt werden soll.
- Wenn die Anzahl der ausgegebenen Objekte in jedem Balken mehr als 20 beträgt oder betragen könnte, sind Stapeldiagramme nicht empfehlenswert.

Mehrfarbige Diagramme

Wenn Sie eine Gruppierung anhand von mehreren Feldern und Zeitreihen erstellen, erstellt Log Insight ein mehrfarbiges Diagramm. Das Diagramm besteht aus zwei untereinander abwechselnden Farben. Jeder Farbwechsel stellt einen neuen Zeitraum dar. Die Interpretation von mehrfarbigen Diagrammen kann schwierig sein. Überlegen Sie sich daher, wie relevant das Diagramm ist, bevor Sie es in ein Inhaltspaket aufnehmen.

Wenn Sie eine Gruppierung nach mehreren Feldern vornehmen, sollten Sie die Verwendung von nicht zeitbasierten Reihen in Betracht ziehen. Durch das Entfernen der Zeitreihe wird ein Balkendiagramm übersichtlicher.

Wenn mehrere Felder in einem bestimmten Zeitbereich wichtig sind, können Sie mehrere einzelne Diagramme für jedes Feld im Zeitbereich erstellen. Sie können die Diagramme dann in derselben Spalte einer Dashboard-Gruppe in einem Inhaltspaket anzeigen.

Meldungsabfragen

Beim Aufbau einer Zusammenfassungsabfrage sollte die Meldungsabfrage nur Ergebnisse ausgeben, die für die Zusammenfassungsabfrage von Relevanz sind. Dies vereinfacht die Analyse und gewährleistet, dass in den Ergebnissen nur relevante Felder aufgeführt werden. Damit die Meldungsabfrage dieselben Ergebnisse ausgibt wie die Zusammenfassungsabfrage, müssen Sie Einschränkungen mit dem Operator *ist vorhanden* für jedes Feld erstellen, das in der Zusammenfassungsabfrage verwendet wird.

Warnungen

Warnungen bieten eine Möglichkeit, eine Reaktion auszulösen, wenn ein bestimmter Ereignistyp eintritt.

Log Insight unterstützt zwei Arten von Warnungen

- E-Mail

- vRealize Operations Manager

Sie können Warnungen nur in einem Benutzerspeicher speichern. Standardmäßig sind alle Inhaltspaket-Warnungen deaktiviert. Wenn Sie eine aktivierte Warnung erstellen und sie als Teil eines Inhaltspakets exportieren, wird die Warnung in dem Inhaltspaket deaktiviert.

Inhaltspakete enthalten keine E-Mail- und vRealize Operations Manager-Einstellungen. Sie können diese Einstellungen auch nicht zu einem Inhaltspaket hinzufügen.

Schwellenwerte

Schwellenwerte begrenzen die Anzahl der ausgelösten Warnungen.

Es ist wichtig, dass Sie die Funktionsweise von Schwellenwerten kennen, damit eine Inhaltspaketwarnung bei aktivierten Schwellenwerten den Benutzer nicht aus Versehen mit Spam überhäuft. Bei der Erwägung der Verwendung eines Schwellenwerts müssen Sie zwei Fragen beachten:

- Wie häufig soll die Warnung ausgelöst werden? Log Insight wird mit vordefinierten Häufigkeiten geliefert. Warnungen werden für das jeweilige Schwellenwertfenster nur ein Mal ausgelöst.
- Wie oft soll überprüft werden, ob ein Warnungszustand eingetreten ist? Eine Warnung wird von einer Abfrage ausgelöst. Warnungen, z. B. Abfragen, werden in der aktuellen Version nicht in Echtzeit ausgelöst. Für jedes Schwellenwertfenster wird eine vordefinierte Abfragehäufigkeit zugeteilt. Wenn der Schwellenwert geändert wird, ändert sich auch die Abfragezeit.

Gruppierungen

Wenn Sie eine E-Mail-Warnung erstellen, müssen Sie nach einem Feld gruppieren, das die Quelle der Warnung identifiziert.

Die von der Warnung gesendete E-Mail enthält eine Tabelle mit Ergebnissen für eine bestimmte Zusammenfassungsabfrage. Die visuelle Darstellung der Abfrage wird auf der Seite „Interaktive Analyse“ angezeigt.

Ohne einen zu gruppierenden eindeutigen Bezeichner wissen Sie nicht, ob das Ergebnis für ein oder mehrere Systeme in Ihrer Umgebung relevant ist. Sie sollten nach dem Feld für den Hostnamen und nicht nach dem Feld für die Quelle gruppieren. Sie können ebenfalls alle Felder hinzufügen, die eindeutig identifizieren, woher das Ereignis stammt.

Empfehlenswerte Praktiken für Dashboard-Gruppen

Dashboard-Gruppen sind in den Inhaltspaketen enthalten. Beim Erstellen von Dashboard-Gruppen sind bestimmte bewährte Praktiken empfehlenswert.

Beim Erstellen von Dashboard-Gruppen sollten die folgenden bewährten Praktiken angewandt werden:

- Inhaltspakete enthalten in der Regel mindestens drei Dashboard-Gruppen. Es empfiehlt sich, am besten mit einer Übersichts-Dashboard-Gruppe zu beginnen, um allgemeine Informationen über die Ereignisse für ein bestimmtes Produkt oder eine bestimmte Anwendung anzugeben. Zusätzlich zu der Übersichts-Dashboard-Gruppe sollten Dashboard-Gruppen anhand von logischen Gruppierungen von Ereignissen erstellt werden. Die logischen Gruppierungen sind produkt- oder anwendungsspezifisch, aber bestimmte allgemeine Vorgehensweisen basieren auf Leistung, Fehlern und Überprüfung. Häufig werden auch Dashboard-Gruppen für eine Komponente erstellt, z. B. für Festplatte und Steuergerät. Bei der komponentenbasierten Vorgehensweise müssen Sie unbedingt beachten, dass diese nur effektiv ist, wenn Abfragen konstruiert werden können, die Ergebnisse von bestimmten Komponenten ausgeben. Falls dies nicht möglich ist, so empfiehlt sich stattdessen der logische Ansatz.
- Achten Sie beim Benennen von Dashboard-Gruppen darauf, dass der Titel möglichst allgemein ist, und fügen Sie nur dann produkt- oder anwendungsspezifische Namen hinzu, wenn die Dashboard-Gruppen in einem komponentenspezifischen Kontext verwendet werden. Beispiel: Das Inhaltspaket VMware vSphere enthält eine Dashboard-Gruppe mit der Bezeichnung ESX/ESXi statt VMware ESX/ESXi.

- Eine Dashboard-Gruppe muss mindestens drei und höchstens sechs Dashboard-Widgets enthalten. Bei weniger als drei Dashboard-Widgets erzielen die von der Dashboard-Gruppe erfassten Informationen nur ein minimales Maß an Aussagekraft. Wenn viele Dashboard-Gruppen vorhanden sind, die nur eine geringe Anzahl von Dashboard-Widgets aufweisen, besteht außerdem das Problem, dass der Benutzer zwischen verschiedenen Seiten wechseln muss und die Informationen nicht in kohärenter Weise präsentiert bekommt.

  Umgekehrt können mehr als sechs Dashboard-Widgets für eine Dashboard-Gruppe negative Auswirkungen haben. Möglicherweise erhalten Sie zu viele, unübersichtliche Informationen. Zu viele Widgets erfordern eine intensive Nutzung Ihrer Systemressourcen, da jedes Widget eine Abfrage ist, die beim System ausgeführt werden muss.

  Wenn Sie mehr als sechs Dashboard-Widgets in eine Dashboard-Gruppe aufnehmen, müssen Sie die Informationen aufteilen und mehrere Dashboard-Gruppen erstellen. Wenn ein Dashboard-Widget für eine oder mehrere Dashboard-Gruppen gültig ist, erstellen Sie das Widget in jeder entsprechenden Dashboard-Gruppe.

Dashboard-Widgets

Mit Dashboard-Widgets können Sie Informationen visualisieren.

Es gibt zwei verschiedene Arten von Dashboard-Widgets in Log Insight:

- ein Diagramm-Widget, das eine visuelle Darstellung von Ereignissen mit einer Verknüpfung zu einer gespeicherten Abfrage enthält,
- eine Abfrageliste, die Titelverknüpfungen zu gespeicherten Abfragen enthält.

Diagramm

Ein Dashboard-Diagramm-Widget enthält eine visuelle Darstellung der Ereignisse. Sie können ein Diagramm als Balken- oder Liniendiagramm darstellen, wobei beide auch in gestapelter Form dargestellt werden können.

Es gibt diverse Möglichkeiten für die Darstellung von Diagrammen:

- Diagramme können viele Informationen enthalten. Eine einzelne Zeile sollte nach Möglichkeit nicht mehr als zwei Diagramm-Widgets enthalten. In einigen seltenen Fällen können drei Diagramm-Widgets effektiv verwendet werden, aber es wird unbedingt davon abgeraten, mehr als drei Diagramm-Widgets in einer Zeile zu verwenden. Bei der Entscheidung darüber, ob Diagramm-Widgets lesbar sind oder nicht, müssen Sie darauf achten, die von Log Insight unterstützte Mindestauflösung von 1024 x 768 Pixel zu verwenden.
- Wenn eine Zeile (außer der letzten Zeile) nur ein Diagramm-Widget enthält, sollte dieses auf der vollen Breite angezeigt werden.
- Verwenden Sie beim Benennen eines Diagramm-Widgets einen beschreibenden Titel und vermeiden Sie unverständliche Feldnamen. Beispielsweise heißt ein extrahiertes Feld `vmw_error_message`. Anstatt ein Diagramm als „`vmw_error_message`-Anzahl“ zu benennen, nennen Sie es lieber „Anzahl der Fehlermeldungen“.
- Sie können ähnliche Diagramme in derselben Dashboard-Gruppe speichern und in derselben Spalte einer Dashboard-Gruppe stapeln, um die visuelle Vergleichbarkeit zu ermöglichen. Beispiel:
  - Durchschnittlich x Ereignisse im Zeitraum + Maximal x Ereignisse im Zeitraum. Die y-Achse der Diagramme weist möglicherweise einen unterschiedlichen Maßstab auf, da unterschiedliche Funktionen verwendet werden.
  - Anzahl der Ereignisse im Zeitraum, gruppiert nach x, + Anzahl der Ereignisse im Zeitraum, gruppiert nach y.

Abfrageliste

Ein Dashboard-Abfragelisten-Widget enthält einen oder mehrere Links zu vordefinierten Abfragen.

Sie können Abfragelisten-Widgets aus folgenden Gründen verwenden:

- Wenn ein Diagramm-Widget an sich keine bedeutende Aussagekraft hat, die zugrunde liegende Abfrage hingegen durchaus.
- Zum Speichern komplexer Abfragen, z. B. Abfragen, die reguläre Ausdrücke verwenden.
- Zur Verwendung verschiedener Zusammenfassungen für dieselbe zugrunde liegende Abfrage innerhalb einer Dashboard-Gruppe.

Fehler beim Importieren von Inhaltspaketen

Wenn Sie ein Inhaltspaket importieren, erhalten Sie möglicherweise Warnungen oder Fehlermeldungen.

Upgrade

Möglicherweise erhalten Sie eine Upgrade-Meldung. Diese bedeutet, dass ein anderes Inhaltspaket mit demselben Namespace auf dem System installiert ist. In diesem Fall können Sie entweder ein Upgrade für das vorhandene Inhaltspaket durchführen und dieses ersetzen, oder Sie können den Upgrade-Vorgang abbrechen und das vorhandene Inhaltspaket beibehalten.

Ungültiges Format

Möglicherweise erhalten Sie eine Meldung, die angibt, dass das Format ungültig ist. Dies bedeutet, dass die VLCP-Datei manuell bearbeitet wird und Syntaxfehler enthält. Die Syntaxfehler müssen vor dem Importieren des Inhaltspakets behoben werden.

Neuere Version

Diese Art der Meldung bedeutet, dass das Inhaltspaket erstellt wird und nur in einer neueren Version von Log Insight unterstützt wird. Wenn Sie auf einer höheren Produktversion als Log Insight 1.5 diese Art der Meldung sehen, bedeutet dies, dass die VLCP-Datei manuell bearbeitet wird.

Unbekannte Version

Wenn die VLCP-Datei manuell bearbeitet wird und Syntaxfehler enthält, wird möglicherweise eine Meldung von diesem Typ angezeigt. Sie müssen die Syntaxfehler beheben, bevor Sie das Inhaltspaket importieren.

HINWEIS Sie sollten die VLCP-Dateien nicht manuell bearbeiten, da dies das Auffinden und Beheben von Syntaxfehlern erschwert.

Anforderungen für das Veröffentlichen von Inhaltspaketen

Achten Sie beim Erstellen und Veröffentlichen eines Inhaltspakets darauf, dass dieses die allgemeinen Anforderungen für die Veröffentlichung erfüllt.

Sie müssen sowohl die Anforderungen für Inhaltspakete als auch die Anforderungen für Veröffentlichungen überprüfen.

Anforderungen für Inhaltspakete

Inhaltspakete müssen bestimmte Anforderungen an Inhalt, Qualität und Standards erfüllen.

Anforderungen an die Inhalte:

- Mindestens drei Dashboard-Gruppen

- Mindestens drei Dashboard-Widgets pro Dashboard-Gruppe
- Höchstens sechs Dashboard-Widgets pro Dashboard-Gruppe
- Höchstens drei Dashboard-Widgets pro Zeile
- Mindestens fünf Warnungen
- Mindestens zwanzig extrahierte Felder

Qualitätsanforderungen an Inhaltspakete:

- Jede Abfrage enthält mindestens ein Volltext-Schlüsselwort und idealerweise mindestens drei Schlüsselwörter
- Abfragen basieren nicht auf umgebungsspezifischen Attributen wie Quelle, Hostname oder *local**.
- Jedes Feld enthält mindestens ein Volltext-Schlüsselwort und idealerweise mindestens drei Schlüsselwörter.
- Felder sind produkt-/anwendungsspezifisch und geben keine Ergebnisse für die Protokolle von anderen Produkten/Anwendungen aus.
- Jedes Dashboard-Widget muss Informationen/Links zu den Anzeigeinhalten des Diagramms und dazu, warum diese wichtig sind, enthalten.

In Bezug auf die Standards für das Erstellen von Inhaltspaketen gelten die folgenden Regeln:

Teil des Inhaltspakets	Formatieren
Namensformat des Inhaltspakets	*Firma-Produkt*
Namespace-Format des Inhaltspakets (Inhaltspaket muss mit Namespace exportiert werden)	*Ext,Domäne,Produkt*
Format des extrahierten Felds	*Präfix_Feld_Name*

Anforderungen für Veröffentlichungen

Überprüfen Sie vor der Veröffentlichung eines Inhaltspakets, ob dieses die Anforderungen für Veröffentlichungen erfüllt.

Anforderung für Veröffentlichungen	Beschreibung
Dateiformat des Inhaltspakets	`VLCP`-Datei.
Ereignisse	Die für die Validierung des Inhaltspakets erforderlichen und geeigneten Ereignisse.
Überblick	Überblick über das Inhaltspaket.
Highlights	Eine Liste, die die Aussagekraft des Inhaltspakets hervorhebt.
Beschreibung	Eine detaillierte Beschreibung der Aussagekraft des Inhaltspakets.
Technische Spezifikationen	Beschreibung der Systemvoraussetzungen.
Video	Beispiel dafür, wie mit dem Inhaltspaket nützliche Erkenntnisse gewonnen werden können.
Whitepaper	Anleitung zum Konfigurieren des Produkts oder der Anwendung, damit Protokolle an Log Insight weitergeleitet werden.

Einsenden eines Inhaltspakets

Senden Sie das Inhaltspaket ein, das Sie auf VMware Solutions Exchange erstellt haben.

Voraussetzungen

- Überprüfen Sie, ob Ihr Inhaltspaket die „Anforderungen für das Veröffentlichen von Inhaltspaketen“, auf Seite 45 erfüllt.
- Wenn Sie kein Konto auf http://solutionexchange.vmware.com haben, klicken Sie auf **Register** und wählen Sie **Partner** aus. Füllen Sie das Registrierungsformular für Partner aus und senden Sie es ab. Sie erhalten eine E-Mail-Benachrichtigung, wenn Ihr Anmeldeantrag genehmigt wurde.

Vorgehensweise

1. Rufen Sie die Seite http://solutionexchange.vmware.com auf und klicken Sie oben rechts auf der Seite auf **Jetzt anmelden**.
2. Geben Sie Ihren Benutzernamen und Ihr Passwort ein und klicken Sie auf **Jetzt anmelden**.
3. Klicken Sie auf **Administration** und wählen Sie **Manage Solutions**, um eine Lösung hinzuzufügen oder zu bearbeiten.
4. Klicken Sie auf **Add Solution** und füllen Sie das Formular mit den erforderlichen Angaben aus.

   Verwenden Sie die Schaltfläche **Save Draft** häufig, damit Ihre Angaben nicht gelöscht werden.
5. Klicken Sie auf **Submit for Approval**.

   Ihre Lösung wird zur Überprüfung und Genehmigung an das VMware Solution Exchange Alliance Team gesendet.

Sie erhalten eine E-Mail mit dem Genehmigungsstatus Ihrer Lösung.

Weiter

Weitere Informationen über die Aufnahme einer Lösung in die Liste erhalten Sie mit einem Klick auf den Link **Partner Corner** oben auf der Seite. Falls Sie die benötigten Informationen nicht finden, wenden Sie sich bei Fragen bitte an VSXAlliance@vmware.com.

Warnungsabfragen in Log Insight

Sie können Log Insight für die Ausführung spezifischer Abfragen in geplanten Intervallen konfigurieren.

Wenn die Anzahl der Ereignisse, die mit der Abfrage übereinstimmen, Ihre eingestellten Schwellenwerte überschreitet, kann Log Insight in vRealize Operations Manager E-Mail-Benachrichtigungen senden und Benachrichtigungsereignisse auslösen.

Navigieren Sie zum Anzeigen der Liste verfügbarer Warnungen zur Seite „Interaktive Analyse“ und wählen Sie im Dropdown-Menü neben der Schaltfläche **Suchen** die Option **Warnungen verwalten** aus. Der Status der einzelnen Warnungen wird jeweils unter dem Namen der Warnung angezeigt.

Hinweis Warnungsabfragen sind benutzerspezifisch. Sie können nur Ihre eigenen Warnungen verwalten.

Arten von Warnungen, die Sie in Log Insight erstellen können

Sie können die Intervalle steuern, in denen die Warnungsabfragen ausgeführt werden. Sie können auch die Bedingungen steuern, unter denen Log Insight Warnungsbenachrichtigungen sendet. Wählen Sie dazu einen der Warnungstypen aus.

Warnung für jeden beliebigen Treffer

Die Warnungsabfrage wird automatisch alle fünf Minuten ausgeführt. Wenn mindestens ein Ereignis innerhalb der letzten 5 Minuten mit der Abfrage übereinstimmt, wird eine Benachrichtigung ausgelöst.

Warnung aufgrund der Anzahl der Ereignisse innerhalb eines benutzerdefinierten Zeitraums

Die Warnungsabfrageintervalle hängen von Ihren Einstellungen ab: Je nach Ihren Einstellungen wird eine Benachrichtigung ausgelöst, wenn in den letzten *y* Minuten mehr oder weniger als *x* übereinstimmende Ereignisse aufgetreten sind.

Wenn dieser Warnungstyp ausgelöst wird, wird er während seines Zeitraums vorübergehend ausgesetzt, um zu verhindern, dass Warnungen für dieselbe Ereignisgruppe doppelt ausgelöst werden. Wenn Sie eine Warnung aktivieren möchten, während sie vorübergehend ausgesetzt ist, können Sie die Warnung deaktivieren und erneut aktivieren.

Warnung aufgrund von Diagrammwerten

Die Warnungsabfrage löst eine Benachrichtigung aus, wenn in dem von Ihnen angegebenen Zeitraum mindestens ein Balken im Diagramm über oder unter dem eingestellten Schwellenwert liegt.

Dieser Warnungstyp kann für Diagramme eingestellt werden, die nicht die **Anzahl** von Ereignissen **über einen Zeitraum** darstellen.

Inhaltspaket-Warnungen

Inhaltspakete können Warnungsabfragen enthalten. Das in Log Insight standardmäßig enthaltene vSphere-Inhaltspaket enthält diverse vordefinierte Warnungsabfragen. Diese können Warnungen auslösen, wenn ein ESXi-Host keine Syslog-Daten mehr sendet, wenn Log Insight keine Ereignisse, Aufgaben und Warnungsdaten von einem vCenter Server mehr erfassen kann oder wenn sich ein Warnungsstatus in Rot ändert. Sie können diese Warnungsabfragen als Vorlagen zum Erstellen von Warnungen verwenden, die spezifisch auf Ihre Umgebung zugeschnitten sind.

Alle Inhaltspaket-Warnungen sind standardmäßig deaktiviert.

Die Warnung **vCenter Server: Lesen der Protokollierungsdaten von ESX/ESXi unterbrochen** zu aktivieren ist eine gute Praxis, weil bestimmte Versionen von ESXi-Hosts das Senden von Syslog-Daten möglicherweise unterbrechen, wenn Sie Log Insight neu starten. Diese Warnung achtet bei der Überwachung auf das vCenter Server-Ereignis `esx.problem.vmsyslogd.remote.failure`, um zu ermitteln, ob ein ESXi-Host das Senden von Syslog-Feeds unterbrochen hat. Weitere Informationen zu Syslog-Problemen und -Lösungen, sieheVMware ESXi 5.x-Host sendet keine Syslogs mehr an den Remote-Server (2003127).

Sie können die folgenden Filter zu der Warnungsabfrage hinzufügen und sie als neue Warnung speichern, um nur ESXi-Hosts zu erfassen, die das Senden von Feeds an Ihre Instanz von Log Insight unterbrechen: **vc_remote_host (VMware – vSphere) enthält** *log-insight-hostname*.

Warnungsabfragen in Inhaltspaketen sind schreibgeschützt. Damit Sie Änderungen in einer Warnung aus einem Inhaltspaket speichern können, müssen Sie die Warnung in Ihrem benutzerdefinierten Inhalt speichern.

- Hinzufügen einer Warnungsabfrage in Log Insight zum Senden von E-Mail-Benachrichtigungen auf Seite 49

  Sie können Warnungsabfragen in Log Insight konfigurieren, um E-Mail-Benachrichtigungen zu senden, wenn bestimmte Daten in den Protokollen vorkommen.

- Hinzufügen einer Warnungsabfrage in Log Insight zum Senden von Benachrichtigungsereignissen an vRealize Operations Manager auf Seite 50

  Sie können Warnungsabfragen in Log Insight konfigurieren, damit Benachrichtigungsereignisse an vRealize Operations Manager gesendet werden, wenn spezifische Log Insight-Abfragen Ergebnisse ausgeben, die über einem bestimmten Schwellenwert liegen.

- Anzeigen von vorhandenen Warnungsabfragen auf Seite 53

  Sie können die Alarmabfragen anzeigen, die Sie erstellt haben, und prüfen, ob die Benachrichtigungen für diese Abfragen aktiviert sind.

- Bearbeiten einer Warnungsabfrage auf Seite 53

  Sie können den Auslöser einer gespeicherten Warnungsabfrage ändern und die von der Abfrage gesendeten Benachrichtigungen aktivieren oder deaktivieren.

- Aktivieren einer Warnungsabfrage auf Seite 54

  Wenn eine Warnungsabfrage deaktiviert wird, sendet Log Insight keine E-Mail-Benachrichtigungen und löst keine vRealize Operations Manager-Benachrichtigungsereignisse aus.

- Löschen einer Warnungsabfrage auf Seite 56

  Sie können Warnungsabfragen löschen, wenn Sie diese nicht mehr benötigen.

Hinzufügen einer Warnungsabfrage in Log Insight zum Senden von E-Mail-Benachrichtigungen

Sie können Warnungsabfragen in Log Insight konfigurieren, um E-Mail-Benachrichtigungen zu senden, wenn bestimmte Daten in den Protokollen vorkommen.

Voraussetzungen

- Vergewissern Sie sich, dass Sie bei der Web-Benutzeroberfläche von Log Insight angemeldet sind. Das URL-Format lautet https://*log_insight-host*, wobei *log_insight-host* die IP-Adresse oder der Hostname der virtuellen Log Insight-Appliance ist.
- Vergewissern Sie sich, dass ein Administrator SMTP zur Aktivierung von E-Mail-Benachrichtigungen konfiguriert hat. Weitere Informationen finden Sie im Thema *Konfigurieren des SMTP-Servers für Log Insight* im Log Insight-Administratorhandbuch.

Vorgehensweise

1. Führen Sie in der Registerkarte **Interaktive Analyse** die Abfrage aus, für die Benachrichtigungen gesendet werden sollen.
2. Klicken Sie im Menü rechts neben der Schaltfläche **Suchen** auf und wählen Sie **Warnung aus Anfrage erstellen...**.
3. Geben Sie im Dialogfeld „Warnung hinzufügen“ einen Namen für die Warnung ein und geben Sie eine kurze, aussagekräftige Beschreibung des Ereignisses an, das die Warnung auslöst.

   Der Name und die Beschreibung der Warnung werden in die von Log Insight gesendete E-Mail aufgenommen.
4. Aktivieren Sie das Kontrollkästchen **E-Mail** und geben Sie die E-Mail-Adresse ein, an die Log Insight die Benachrichtigungen senden soll.

   Verwenden Sie Kommas zum Trennen mehrerer Adressen.

5 Stellen Sie den Alarmschwellenwert ein.

Warnungstyp	Auswahl
Alle Übereinstimmungen	Wählen Sie die Option **bei einem beliebigen Treffer**. Abfragen werden alle 5 Minuten ausgeführt.
Basierend auf der Anzahl der Ereignisse innerhalb einer Zeitspanne	Wählen Sie die zweite Option und stellen Sie die Parameter über die Dropdown-Menüs ein. Die Abfragen werden je nach Ihrer Auswahl im zweiten Dropdown-Menü ausgeführt.
Basierend auf Diagrammwerten	Wählen Sie das dritte Optionsfeld und konfigurieren Sie die Parameter über die Dropdown-Menüs. HINWEIS Dieser Warnungstyp ist nur verfügbar, wenn Sie die Gruppierung von Ereignissen nach mindestens einem Feld auswählen. Sie können diesen Warnungstyp nicht für Diagramme erstellen, auf denen nur Zeitserien angezeigt werden. Die Abfragen werden je nach Ihrer Auswahl im zweiten Dropdown-Menü ausgeführt.

Die orangefarbene Linie im Vorschaudiagramm zeigt den Schwellenwert an.

6 Klicken Sie auf **Speichern**.

Weiter

Sie können Ihre gespeicherten Warnungen aktivieren, deaktivieren oder löschen.

HINWEIS Warnungsabfragen sind benutzerspezifisch. Sie können nur Ihre eigenen Warnungen verwalten.

Hinzufügen einer Warnungsabfrage in Log Insight zum Senden von Benachrichtigungsereignissen an vRealize Operations Manager

Sie können Warnungsabfragen in Log Insight konfigurieren, damit Benachrichtigungsereignisse an vRealize Operations Manager gesendet werden, wenn spezifische Log Insight-Abfragen Ergebnisse ausgeben, die über einem bestimmten Schwellenwert liegen.

Von Log Insight generierte Benachrichtigungsereignisse werden mit Ressourcen in vRealize Operations Manager verknüpft. Weitere Informationen über Ressourcen erhalten Sie in der Anleitung *Erste Schritte für vRealize Operations Manager (benutzerdefinierte Benutzeroberfläche)*.

HINWEIS Es dauert mehrere Minuten, bis Benachrichtigungsereignisse in der Benutzeroberfläche von vRealize Operations Manager angezeigt werden.

Voraussetzungen

- Vergewissern Sie sich, dass Sie bei der Web-Benutzeroberfläche von Log Insight angemeldet sind. Das URL-Format lautet https://*log_insight-host*, wobei *log_insight-host* die IP-Adresse oder der Hostname der virtuellen Log Insight-Appliance ist.
- Vergewissern Sie sich, dass ein Administrator die Verbindung zwischen Log Insight und vRealize Operations Manager konfiguriert hat, um die Integration von Warnungen zu aktivieren. Weitere Informationen finden Sie im Thema *Konfigurieren von Log Insight zum Senden von Benachrichtigungsereignissen an vRealize Operations Manager* im Log Insight-Administratorhandbuch.

Vorgehensweise

1 Führen Sie in der Registerkarte **Interaktive Analyse** die Abfrage aus, für die Benachrichtigungen gesendet werden sollen.

2 Klicken Sie im Menü rechts neben der Schaltfläche **Suchen** auf und wählen Sie **Warnung aus Anfrage erstellen...**.

3 Geben Sie im Dialogfeld „Warnung hinzufügen" einen Namen für die Warnung ein und geben Sie eine kurze, aussagekräftige Beschreibung des Ereignisses an, das die Warnung auslöst.

Der Name und die Beschreibung der Warnung werden in das von Log Insight gesendete Benachrichtigungsereignis aufgenommen.

Hinweis Die Beschreibung der Warnung ist nur in der von Log Insight gesendeten E-Mail-Nachricht sichtbar.

4 Deaktivieren Sie das Kontrollkästchen **E-Mail** oder geben Sie mindestens eine E-Mail-Adresse an, um die Benachrichtigungsereignisse zu empfangen.

Verwenden Sie Kommas zum Trennen mehrerer Adressen.

5 Wählen Sie **An vRealize Operations Manager senden** aus.

6 Klicken Sie auf **Auswählen**, um eine vRealize Operations Manager-Ressource auszuwählen, die mit den von Log Insight gesendeten Benachrichtigungsereignissen verknüpft werden soll.

7 Geben Sie im Dialogfeld „vRealize Operations Manager-Ressource für den Erhalt der Warnung auswählen" einen Ressourcennamen ein oder suchen Sie ein Objekt in der Liste.

Mit dem Dropdown-Menü können Sie Ressourcen nach Betriebszustand filtern.

Option	Beschreibung
Aktive VMs	Wählen Sie diese Option, um nur eingeschaltete Ressourcen anzuzeigen .
Alle Ressourcen	Wählen Sie diese Option, um alle Ressourcen unabhängig vom Betriebszustand anzuzeigen.

8 Wählen Sie im Dropdown-Menü **Kritikalität** die Kritikalitätsstufe für die Benachrichtigungsereignisse aus, die in der benutzerdefinierten Benutzeroberfläche von vRealize Operations Manager angezeigt werden.

9 Stellen Sie den Alarmschwellenwert ein.

Warnungstyp	Auswahl
Alle Übereinstimmungen	Wählen Sie die Option **bei einem beliebigen Treffer**. Abfragen werden alle 5 Minuten ausgeführt.
Basierend auf der Anzahl der Ereignisse innerhalb einer Zeitspanne	Wählen Sie die zweite Option und stellen Sie die Parameter über die Dropdown-Menüs ein. Die Abfragen werden je nach Ihrer Auswahl im zweiten Dropdown-Menü ausgeführt.
Basierend auf Diagrammwerten	Wählen Sie das dritte Optionsfeld und konfigurieren Sie die Parameter über die Dropdown-Menüs. **Hinweis** Dieser Warnungstyp ist nur verfügbar, wenn Sie die Gruppierung von Ereignissen nach mindestens einem Feld auswählen. Sie können diesen Warnungstyp nicht für Diagramme erstellen, auf denen nur Zeitserien angezeigt werden. Die Abfragen werden je nach Ihrer Auswahl im zweiten Dropdown-Menü ausgeführt.

Die orangefarbene Linie im Vorschaudiagramm zeigt den Schwellenwert an.

10 Klicken Sie auf **Speichern**.

Wenn die Warnungsabfrage Ergebnisse ausgibt, die mit den Warnungskriterien übereinstimmen, wird ein Benachrichtigungsereignis an vRealize Operations Manager gesendet. Warnungsabfragen werden nach einem vordefinierten Plan ausgeführt und nur einmal für einen bestimmten Zeitschwellenbereich ausgelöst.

Die Benachrichtigungsereignisse werden je nach der verwendeten Benutzeroberfläche von vRealize Operations Manager an unterschiedlichen Stellen angezeigt.

Beispiel: Konfigurieren eines Benachrichtigungsereignisses für vRealize Operations Manager

Angenommen Sie haben in vRealize Operations Manager eine virtuelle Maschinenressource mit dem Namen vm-abc.

Sie haben Log Insight für das Abrufen von Ereignissen von dem vCenter Server-System konfiguriert, auf dem die virtuelle Maschine vm-abc ausgeführt wird.

Sie möchten bei jedem Ausschalten der virtuellen Maschine vm-abc eine Benachrichtigung in vRealize Operations Manager erhalten.

Konfigurieren Sie Log Insight wie folgt, um diese Benachrichtigungsereignisse an vRealize Operations Manager zu senden.

1. Geben Sie im Suchtextfeld `Ausschaltung virtuelle Maschine` ein.
2. Klicken Sie auf **Filter hinzufügen**, wählen Sie **vc_vm_name** und geben Sie `vm-abc` ein.
3. Klicken Sie auf **Suchen**.

   Wenn die virtuelle Maschine vm-abc während des ausgewählten Zeitraums ausgeschaltet wurde, gibt die Suche alle aufgetretenen Instanzen aus.
4. Wählen Sie im Dropdown-Menü rechts von der Schaltfläche **Suchen** die Option **Warnung hinzufügen**.
5. Geben Sie im Dialogfeld „Warnung hinzufügen" einen Namen und eine Beschreibung für die Warnung ein, deaktivieren Sie das Kontrollkästchen **E-Mail** und wählen Sie **An vRealize Operations Manager senden** aus.
6. Klicken Sie auf **Auswählen**, geben Sie `vm-abc` ein und klicken Sie dann auf **Suchen**, um die Ressource vm-abc in der Liste zu suchen.
7. Klicken Sie in der Liste auf die Ressource vm-abc, um sie hinzuzufügen.
8. (Optional) Bearbeiten Sie die Kritikalitätsstufe, die in der benutzerdefinierten Benutzeroberfläche von vRealize Operations Manager angezeigt wird.
9. Wählen Sie unter „Eine Warnung auslösen" die Option **bei jedem beliebigen Treffer**.
10. Klicken Sie auf **Speichern**.

Log Insight fragt das vCenter Server-System in Fünf-Minuten-Intervallen ab. Wenn die Abfrage eine neue VM-Ausschaltungsaufgabe für die VM vm-abc ergibt, sendet Log Insight ein Benachrichtigungsereignis, das mit der Ressource vm-abc in vRealize Operations Manager verknüpft ist.

Weiter

Sie können Ihre gespeicherten Warnungen aktivieren, deaktivieren oder löschen.

HINWEIS Warnungsabfragen sind benutzerspezifisch. Sie können nur Ihre eigenen Warnungen verwalten.

Anzeigen von vorhandenen Warnungsabfragen

Sie können die Alarmabfragen anzeigen, die Sie erstellt haben, und prüfen, ob die Benachrichtigungen für diese Abfragen aktiviert sind.

HINWEIS Warnungsabfragen sind benutzerspezifisch. Sie können nur Ihre eigenen Warnungen verwalten.

Voraussetzungen

Vergewissern Sie sich, dass Sie bei der Web-Benutzeroberfläche von Log Insight angemeldet sind. Das URL-Format lautet https://*log_insight-host*, wobei *log_insight-host* die IP-Adresse oder der Hostname der virtuellen Log Insight-Appliance ist.

Vorgehensweise

1 Rufen Sie die Registerkarte **Interaktive Analyse** auf.

2 Klicken Sie im Menü rechts neben der Schaltfläche **Suchen** auf und wählen Sie **Warnungen verwalten** aus.

Sie sehen eine Liste aller Ihrer Warnungsabfragen. Der Status der Warnungsbenachrichtigungen wird unter dem Namen der Warnung angezeigt.

Weiter

Sie können auf Warnungsabfragen in der Liste klicken, um ihre Parameter zu ändern, oder Sie können die Abfragen löschen, die Sie nicht mehr benötigen.

Warnungsabfragen in Inhaltspaketen sind schreibgeschützt. Damit Sie Änderungen in einer Warnung aus einem Inhaltspaket speichern können, müssen Sie die Warnung in Ihrem benutzerdefinierten Inhalt speichern.

Bearbeiten einer Warnungsabfrage

Sie können den Auslöser einer gespeicherten Warnungsabfrage ändern und die von der Abfrage gesendeten Benachrichtigungen aktivieren oder deaktivieren.

HINWEIS Warnungsabfragen sind benutzerspezifisch. Sie können nur Ihre eigenen Warnungen verwalten.

Warnungsabfragen in Inhaltspaketen sind schreibgeschützt. Damit Sie Änderungen in einer Warnung aus einem Inhaltspaket speichern können, müssen Sie die Warnung in Ihrem benutzerdefinierten Inhalt speichern.

Voraussetzungen

- Vergewissern Sie sich, dass Sie bei der Web-Benutzeroberfläche von Log Insight angemeldet sind. Das URL-Format lautet https://*log_insight-host*, wobei *log_insight-host* die IP-Adresse oder der Hostname der virtuellen Log Insight-Appliance ist.
- Vergewissern Sie sich, dass ein Administrator SMTP zur Aktivierung von E-Mail-Benachrichtigungen konfiguriert hat. Weitere Informationen finden Sie im Thema *Konfigurieren des SMTP-Servers für Log Insight* im Log Insight-Administratorhandbuch.
- Vergewissern Sie sich, dass ein Administrator die Verbindung zwischen Log Insight und vRealize Operations Manager konfiguriert hat, um die Integration von Warnungen zu aktivieren. Weitere Informationen finden Sie im Thema *Konfigurieren von Log Insight zum Senden von Benachrichtigungsereignissen an vRealize Operations Manager* im Log Insight-Administratorhandbuch.

Vorgehensweise

1 Rufen Sie die Registerkarte **Interaktive Analyse** auf.

2 Klicken Sie im Menü rechts neben der Schaltfläche **Suchen** auf und wählen Sie **Warnungen verwalten** aus.

3 Klicken Sie in der Liste „Warnungen“ auf die Warnungsabfrage, die Sie bearbeiten möchten, und ändern Sie die Abfrageparameter nach Bedarf.

HINWEIS Wenn Sie beide Benachrichtigungsoptionen deaktivieren, wird die Warnungsabfrage deaktiviert.

4 Speichern Sie Ihre Änderungen.

Option	Beschreibung
Speichern	Diese Schaltfläche wird angezeigt, wenn Sie Ihre eigenen Warnungen bearbeiten.
In 'Meine Warnungen' speichern	Diese Schaltfläche wird angezeigt, wenn Sie eine freigegebene Warnung oder eine Warnung aus einem Inhaltspaket bearbeiten. Die ursprüngliche Warnung bleibt unverändert, aber Sie speichern eine Kopie der Warnung in Ihrem benutzerdefinierten Inhalt.

Aktivieren einer Warnungsabfrage

Wenn eine Warnungsabfrage deaktiviert wird, sendet Log Insight keine E-Mail-Benachrichtigungen und löst keine vRealize Operations Manager-Benachrichtigungsereignisse aus.

HINWEIS Warnungsabfragen sind benutzerspezifisch. Sie können nur Ihre eigenen Warnungen verwalten.

Eine Warnungsabfrage wird unter den folgenden Bedingungen deaktiviert:

- wenn Sie beide Benachrichtigungsoptionen im Dialogfeld „Warnung bearbeiten“ deaktivieren,
- wenn die Warnung Teil eines Inhaltspakets ist.

Warnungsabfragen in Inhaltspaketen sind schreibgeschützt. Damit Sie Änderungen in einer Warnung aus einem Inhaltspaket speichern können, müssen Sie die Warnung in Ihrem benutzerdefinierten Inhalt speichern.

Voraussetzungen

- Vergewissern Sie sich, dass Sie bei der Web-Benutzeroberfläche von Log Insight angemeldet sind. Das URL-Format lautet https://*log_insight-host*, wobei *log_insight-host* die IP-Adresse oder der Hostname der virtuellen Log Insight-Appliance ist.
- Vergewissern Sie sich, dass ein Administrator SMTP zur Aktivierung von E-Mail-Benachrichtigungen konfiguriert hat. Weitere Informationen finden Sie im Thema *Konfigurieren des SMTP-Servers für Log Insight* im Log Insight-Administratorhandbuch.
- Vergewissern Sie sich, dass ein Administrator die Verbindung zwischen Log Insight und vRealize Operations Manager konfiguriert hat, um die Integration von Warnungen zu aktivieren. Weitere Informationen finden Sie im Thema *Konfigurieren von Log Insight zum Senden von Benachrichtigungsereignissen an vRealize Operations Manager* im Log Insight-Administratorhandbuch.

Vorgehensweise

1 Rufen Sie die Registerkarte **Interaktive Analyse** auf.

2 Klicken Sie im Menü rechts neben der Schaltfläche **Suchen** auf und wählen Sie **Warnungen verwalten** aus.

3 Klicken Sie in der Liste „Warnungen" auf die Warnungsabfrage, die Sie aktivieren möchten.

4 Wählen Sie die Benachrichtigungsoptionen, die Sie aktivieren möchten, und geben Sie die erforderlichen Parameter an.

Option	Beschreibung
E-Mail	Geben Sie mindestens eine E-Mail-Adresse in das Textfeld ein. Verwenden Sie Kommas zum Trennen mehrerer Adressen.
Senden an vRealize Operations Manager	Wählen Sie eine vRealize Operations Manager-Ressource aus, um sie mit den Benachrichtigungsereignissen zu verknüpfen, und wählen Sie die Kritikalitätsstufe der Ereignisse aus.

5 Speichern Sie Ihre Änderungen.

Option	Beschreibung
Speichern	Diese Schaltfläche wird angezeigt, wenn Sie Ihre eigenen Warnungen bearbeiten.
In 'Meine Warnungen' speichern	Diese Schaltfläche wird angezeigt, wenn Sie eine freigegebene Warnung oder eine Warnung aus einem Inhaltspaket bearbeiten. Die ursprüngliche Warnung bleibt unverändert, aber Sie speichern eine Kopie der Warnung in Ihrem benutzerdefinierten Inhalt.

Wenn die Warnungsabfrage Ergebnisse ausgibt, die mit den Warnungskriterien übereinstimmen, sendet Log Insight Ihrer Konfiguration entsprechend Benachrichtigungen.

Beispiel: Eine Warnung aus dem VMware vSphere-Inhaltspaket aktivieren

Das VMware vSphere-Inhaltspaket enthält diverse vordefinierte Warnungsabfragen, darunter die Warnung **vCenter Server: Lesen der Protokollierungsdaten von ESX/ESXi unterbrochen**.

Die Warnung **vCenter Server: Lesen der Protokollierungsdaten von ESX/ESXi unterbrochen** zu aktivieren ist eine gute Praxis, weil bestimmte Versionen von ESXi-Hosts das Senden von Syslog-Daten möglicherweise unterbrechen, wenn Sie Log Insight neu starten. Diese Warnung achtet bei der Überwachung auf das vCenter Server-Ereignis `esx.problem.vmsyslogd.remote.failure`, um zu ermitteln, ob ein ESXi-Host das Senden von Syslog-Feeds unterbrochen hat.

1 Erweitern Sie auf der Registerkarte **Interaktive Analyse** das Dropdown-Menü rechts neben der Schaltfläche **Suchen** und wählen Sie **Warnungen verwalten**.

2 Klicken Sie unter „VMware vSphere-Inhaltspaket" auf **vCenter Server: Lesen der Protokollierungsdaten von ESX/ESXi unterbrochen**.

3 Aktivieren von E-Mail Benachrichtigungen oder vRealize Operations Manager-Benachrichtigungsereignissen

4 Klicken Sie auf **In 'Meine Warnungen' speichern**.

Damit nur ESXi-Hosts erfasst werden, die keine Feeds mehr an Ihre Log Insight-Instanz senden, können Sie den folgenden Filter zur Warnungsabfrage hinzufügen: **vc_remote_host (VMware – vSphere) enthält** *<log-insight-hostname>* . Speichern Sie die neue Abfrage dann unter Ihren Warnungen.

Einzelheiten zu Syslog-Problemen und -Lösungen finden Sie unter VMware ESXi 5.0 host stops sending syslogs to remote server (2003127).

Löschen einer Warnungsabfrage

Sie können Warnungsabfragen löschen, wenn Sie diese nicht mehr benötigen.

HINWEIS Warnungsabfragen sind benutzerspezifisch. Sie können nur Ihre eigenen Warnungen verwalten.

Voraussetzungen

Vergewissern Sie sich, dass Sie bei der Web-Benutzeroberfläche von Log Insight angemeldet sind. Das URL-Format lautet https://*log_insight-host*, wobei *log_insight-host* die IP-Adresse oder der Hostname der virtuellen Log Insight-Appliance ist.

Vorgehensweise

1. Rufen Sie die Registerkarte **Interaktive Analyse** auf.
2. Klicken Sie im Menü rechts neben der Schaltfläche **Suchen** auf und wählen Sie **Warnungen verwalten** aus.
3. Wählen Sie den Namen der Warnung aus, die Sie löschen möchten, und klicken Sie auf das Symbol **Löschen**.
4. Wählen Sie im Dialogfeld **Warnung löschen** den Befehl **Löschen**.

Index